

p -Central Subspaces of Central Simple Algebras

Adam Chapman

Department of Mathematics

Ph.D. Thesis

Submitted to the Senate of Bar-Ilan University

Ramat-Gan, Israel

August 2013

This work was carried out under the supervision of
Prof. Uzi Vishne
Department of Mathematics, Bar-Ilan University.

This thesis is dedicated to the memory of my beloved grandmother Ahuva Luz (née Frenkel), who died of cancer during the first year of my PhD.

Contents

Abstract	i
Introduction	1
Chapter 1. Clifford Algebras	5
1. Background	5
2. The Finite Linearization Problem	8
3. The Clifford Algebra of a Short p -Central Space	13
4. The Clifford Algebra of a Short 4-Central Space	15
5. The Clifford Algebra of a Monic Polynomial	19
6. The Clifford Algebra of a Degree d Projective Variety	29
Chapter 2. d -Central Spaces in Tensor Products of Cyclic Algebras	33
1. Background	33
2. Maximal p -Central Spaces	34
3. Family of p^k -Central Spaces	35
4. 5-Dimensional 4-Central Spaces	36
5. p -Central Spaces containing p -Central Sets of Size 3	39
6. 3-Central Spaces spanned by 3-Central Sets	43
7. Algebras of Fixed Degrees with 3-Central Subspaces	46
Chapter 3. Chain Lemmas	53
1. Background	53
2. Chains of p -Central Elements in p -Cyclic Algebras	54
3. The Chain Lemma for Biquaternion Algebras	64
Chapter 4. Computational Aspects	75
1. Quadratic Elements and Quaternion Standard Equations	75
2. General Polynomials and Left Eigenvalues	82
Bibliography	87

Abstract

We study central simple algebras in various ways, focusing on the role of p -central subspaces. The first part of my thesis is dedicated to the study of Clifford algebras. The standard Clifford algebra of a given form is the generic associative algebra containing a p -central subspace whose exponentiation form is equal to the given form. There is an old question as for whether these algebras have representations of finite rank over the center, and jointly with Daniel Krashen and Max Lieblich we managed to provide a positive answer. Different generalizations of the structure of the Clifford algebra are presented and studied in that part too. The second part is dedicated to the study of p -central subspaces of given central simple algebras, mainly tensor products of cyclic algebras of degree p . Among the results, we prove that 5 is the upper bound for the dimension of 4-central subspaces of cyclic algebras of degree 4 containing pairs of standard generators. The third part is dedicated to chain lemmas. Chain lemmas are of importance in the theory of central simple algebras, because they form one approach to solving the word problem for the Brauer group. We prove the chain lemma for biquaternion algebras, both in characteristic 2 and characteristic not 2, and prove some partial results on the chain lemmas for cyclic algebras of degree p . The fourth part is dedicated to the more computational aspects of the theory. It contains results on quaternion polynomial equations and on left eigenvalues of quaternion matrices.

Introduction

A finite dimensional associative algebra A over a field F is called central simple if it has no proper two-sided ideals and $Z(A) = F$. If A and B are two central simple algebras over F then $A \otimes B$ is also central simple over F . Consequently, the set of isomorphism classes of central simple algebras over F forms a semigroup.

According to Wedderburn, if A is central simple over F then A decomposes uniquely as $M \otimes D$ where M is a matrix algebra over F and D is a central division algebra over F . Both M and D are in particular central simple algebras. We say that A and B are Brauer equivalent if they have the same underlying division algebra. Consequently, the set of central simple algebras over F modulo that equivalence relation forms a commutative monoid.

It is known that $A \otimes A^{\text{op}}$ is a matrix algebra, and therefore this monoid is a group, and is called the Brauer group of F .

This group is known to be a torsion group, i.e. for every central simple algebra A there exists some positive integer e such that $A \otimes \overset{(e \text{ times})}{\dots} \otimes A$ is a matrix algebra over F . The minimal such e is called the exponent of A and denoted by $\exp(A)$.

A splitting field of a given central simple algebra A over F is a field extension K/F for which $A \otimes_F K$ is a matrix algebra over K , i.e. $A \otimes_F K = M_d(K)$ for some integer n . A splitting field is known to exist for any central simple algebra, for example any maximal subfield of the algebra is a splitting field. Since $[A : F] = [A \otimes K : K]$, $[A : F]$ is the square of some integer, called the degree of A and denoted by $\deg(A)$. The degree of the underlying division algebra D of A is called the index of A and is denoted by $\text{ind}(A)$.

It is known that $\exp(A) | \text{ind}(A) | \deg(A)$.

One way to study the structure of a given division or central simple algebra A over some center F is to focus on some subsets of elements with special behavior, such as d -central elements. A noncentral element y is called d -central if y^d is in the center and y^k is not in the center for

any $1 \leq k \leq d - 1$. When d is a prime, we often use the letter p , and refer to these elements as p -central elements.

The d -central elements are of special importance in the structure theory of division algebras and of central simple algebras in general, through their connection to cyclic field extensions and cyclic algebras.

Every maximal subfield of a division algebra has dimension equal to the degree. The algebra is called cyclic if it has a maximal subfield which is cyclic Galois over the center.

Hamilton's quaternion algebra is the classical example of a cyclic algebra of degree 2 over the real numbers. The first examples of arbitrary degree were constructed by Dickson [Dic14], as follows: Let L/F be an n -dimensional cyclic Galois extension with σ a generator of $\text{Gal}(L/F)$, and let $\beta \in F^\times$. Then $\bigoplus_{i=0}^{p-1} Ly^i$, subject to the relations $yu = \sigma(u)y$ (for $u \in L$) and $y^n = \beta$, is a cyclic algebra of degree d , denoted by $(L/F, \sigma, \beta)$; every cyclic algebra has this form. In particular, every cyclic algebra of degree d has a d -central element.

If F contains a primitive d th root of unity, then each d -central element of a division algebra generates a cyclic maximal subfield. However, there are central division algebras with d -central elements which are not cyclic. The first example, for $d = 4$, was given by Albert, and an example with $n = q^2$ for an arbitrary prime q was recently constructed by Matzri, Rowen and Vishne [MRV12]. Nevertheless, Albert proved that if p is prime then every central division algebra with a p -central element is cyclic, regardless of the characteristic of the field or the existence of a primitive p th root of unity.

For prime d , when F is of characteristic prime to d and contains a primitive d th root of unity ρ , a cyclic maximal subfield has the form $L = F[x]$ where x is d -central, so every cyclic algebra has the 'symbol algebra' form

$$(\alpha, \beta)_{d,F} = F[x, y : x^d = \alpha, y^d = \beta, yx = \rho xy]$$

emphasizing even further the role of d -central elements in presentations of cyclic algebras.

For prime p , if F is of characteristic p then every cyclic algebra of degree p over F has the form

$$(\alpha, \beta)_{p,F} = F[x, y : x^p - x = \alpha, y^p = \beta, yx - xy = y].$$

In this case, along the p -central elements there are also the Artin-Schreier elements, i.e. non-central elements satisfying the condition $x^p - x \in F$.

A d -central space V is an F -vector subspace of A in which all the nonzero elements are d -central. For example, in the above presentation, $Fx + Fy$ is a d -central space. Furthermore, $Fx + F[x]y$ is d -central. The existence of p -central spaces tells us a lot about the structure of the algebra as we shall soon see.

The decomposition of elements with respect to a given special element also stars throughout this thesis. For characteristic prime to d , we use the eigenvector decomposition of elements with respect to conjugation by a certain d -central element.

LEMMA 0.1. *In a given associative algebra A over a field F of characteristic prime to d containing a primitive d th root of unity ρ , if $x^d \in F^\times$ then for every $y \in A$, $y = y_0 + \cdots + y_{d-1}$ such that $y_k x = \rho^k x y_k$.*

PROOF. This is the eigenvector decomposition: Take $y_k = \frac{1}{d}(y + \rho^k x y x^{-1} + \cdots + \rho^{k(d-1)} x^{d-1} y x^{1-d})$ for $0 \leq k \leq d-1$. It is an easy calculation to see that $y_k x = \rho^k x y_k$. \square

For a prime p , and characteristic p , there are two interesting types of elements, the Artin-Schreier elements, i.e. elements that satisfy an equation of the form $x^p - x = \alpha$ for some $\alpha \in F$, and p -central elements that are defined above, regardless of the characteristic. In this case, however, the p -central elements generate purely inseparable field extensions over the base-field, while the Artin-Schreier elements generate Galois field extensions.

There are still decomposition lemmas with respect to these two special types of elements.

When the characteristic is p , we write $[\mu, \nu] = [\mu, \nu]_1 = \nu\mu - \mu\nu$ and define $[\mu, \nu]_k$ inductively as $\nu[\mu, \nu]_{k-1} - [\mu, \nu]_{k-1}\nu$. $[\mu, \nu]_0$ is defined to be μ .

LEMMA 0.2. *Given an associative algebra A over a field F of characteristic p , if x is Artin-Schreier then for any $z \in A$, $z = z_0 + z_1 + \cdots + z_{p-1}$ where $[z_k, x] = kz_k$. Similarly, by taking $t_{p-k} = z_k$, $z = t_0 + \cdots + t_{p-1}$ such that $[x, t_k] = kt_k$.*

PROOF. Let $z_0 = z - [z, x]_{p-1}$, and for all $1 \leq k \leq p-1$, $z_k = -(k^{-(p-2)}[z, x]_1 + \cdots + k^{-1}[z, x]_{p-2} + [z, x]_{p-1})$. It is an easy calculation to prove that $[z, x] = kz_k$. It is obvious that $z_0 + z_1 + \cdots + z_{p-1} = z$. \square

LEMMA 0.3. *Given an associative algebra A over a field F of characteristic p , if y is p -central then for any $z \in A$, there exist $\{z_k : k \in \mathbb{Z}_p\}$ such that for all $k \neq 0$, $[z_k, y]_1 = z_{k-1}$ and $[z_0, y]_1 = 0$, and $z = z_{p-1} - z_{p-2}$.*

PROOF. For $k \neq 0$, let $z_k = [z, y]_{p-1-k} + [z, y]_{p-k} + \cdots + [z, y]_{p-1}$.
Let $z_0 = [z, y]_{p-1}$. It is clear that they satisfy the requirements. \square

CHAPTER 1

Clifford Algebras

1. Background

Let F be an infinite field and $f(a_1, \dots, a_n)$ be a homogeneous form of degree d with n variables over F .

The Clifford algebra of f , denoted by C_f , is defined to be

$$F \langle x_1, \dots, x_n : (a_1x_1 + \dots + a_nx_n)^p = f(a_1, \dots, a_n) \forall a_1, \dots, a_n \in F \rangle.$$

This definition is due to Roby [Rob69].

Even though it looks like the number of relations is infinite, C_f is finitely presented.

In [Rev77], Revoy introduced the following notation in order to describe the finite set of relations: $x_1^{d_1} * x_2^{d_2} * \dots * x_n^{d_n}$. This expression means the sum of all the words that consist of only the letters x_1, \dots, x_n and each letter x_i appears exactly d_i times. For example, $x^2 * y = x^2y + yx^2$.

The Clifford algebra is then the algebra generated over F by x_1, \dots, x_n subject to the following relations:

$$x_1^{d_1} * \dots * x_n^{d_n} = \alpha_{d_1, \dots, d_n}$$

for any set of non-negative integers $\{d_1, \dots, d_n\}$ such that $d_1 + \dots + d_n = d$, where α_{d_1, \dots, d_n} is the coefficient of $a_1^{d_1} \dots a_n^{d_n}$ in $f(a_1, \dots, a_n)$.

This algebra is clearly invariant under any linear change of the variables of f , and it is one of the most important invariants of homogeneous forms in general and of quadratic forms in particular. For nondegenerate quadratic forms, the Clifford algebra is a cohomological invariant (see [KMRT98]).

Given a central simple algebra A over F , if A contains a d -central space $V = Fv_1 + \dots + Fv_n$ with a fixed basis $\{v_1, \dots, v_n\}$ then V has a natural exponentiation form $f(a_1, \dots, a_n) = (a_1v_1 + \dots + a_nv_n)^d$. This is a homogeneous form of degree d , and it has a Clifford algebra C_f . One can refer to C_f as the Clifford algebra of the d -central space V itself and denote it by $C(V)$.

The elements of V generate a subalgebra $F[V] = F[v_1, \dots, v_n]$ of A , which is often equal to A . This subalgebra is a finite representation of the Clifford algebra of V . Therefore studying the finite representations of $C(V)$, and in particular its simple images, may shed some light on the structure of A itself.

REMARK 1.1. *Throughout this chapter, by a finite representation of C_f (or $C(V)$) we mean a homomorphic image of C_f inside some matrix algebra of finite degree over F . We say that C_f is finitely representable if such a representation exists. The existence of such a representation is equivalent to the existence of simple images of finite dimension. The rank of a representation is its dimension over F . If a representation is simple its degree is the square root of its rank.*

Every d -central subspace of a central simple algebra has an exponentiation form which is a homogeneous form of degree d . A natural question would be whether every homogeneous form of degree d is the exponentiation form of some d -central subspace of a central simple algebra. This question is known as the “Finite Linearization Problem” and is discussed in Section 2 where a positive answer is provided.

According to Van den Bergh, the Clifford algebra of a binary form of degree ≥ 4 has representations of unbounded high ranks. However, it is not easy to construct explicit examples of high degree simple representations. We provide explicit examples of simple images of degree d^2 and index d for the Clifford algebra of a diagonal binary form of degree d .

The Clifford algebra of a quadratic form or a quadratic space in characteristic not 2 is a classical object. This algebra is known to be a tensor product of quaternion algebras either over F or over a quadratic extension of the center (see, e.g. [Lam73] or [KMRT98]).

The case of $\text{char}(F) = 2$ was studied by Mammone, Tignol and Wadsworth in [MTW91]. They concluded, similarly to the characteristic not 2 case, that the Clifford algebra is a tensor product of quaternion algebras either over F or over a purely inseparable field extension of it.

Assuming $\text{char}(F) \neq 2, 3$, the case of $d = 3$ and $n = 2$ was first considered by Heerema in [Hee54]. Haile studied these algebras in [Hai84] and [Hai92], and showed that C_f is an Azumaya algebra, whose center is isomorphic to the coordinate ring of the affine elliptic curve $s^2 = r^3 - 27\Delta$ where Δ is the discriminant of f . He also proved that the simple homomorphic images of C_f are cyclic algebras of degree 3. Moreover, for every algebraic extension K/F there is a one to one

correspondence between the K -points on that elliptic curve and the simple homomorphic images of C_f whose center is K .

In Section 3 we generalize this result for any prime p , proving that some specific quotient of the Clifford algebra (that is equal to the Clifford algebra in case of $p = 3$) is Azumaya whose center is a hyperelliptic curve and all its simple images are cyclic of degree 3. This is the Clifford algebra of a short p -central space of type $\{i, p - i\}$. Clifford algebras of short p -central spaces of different types appear to have simple images of degree p^2 that are easy to construct.

In [Pap00], Pappacena generalized the notion of the Clifford algebra to the algebra associated to a monic polynomial (with respect to the first variable) the form $\Phi(z, a_1, \dots, a_n) = z^d - \sum_{k=1}^d f_k(a_1, \dots, a_n)z^{d-k}$ where each f_k is a homogeneous form of degree k . This algebra, denoted there by C_Φ , is defined to be

$$\begin{aligned} F\langle x_1, \dots, x_n : (a_1x_1 + \dots + a_nx_n)^d \\ = f_1(a_1, \dots, a_n)(a_1x_1 + \dots + a_nx_n)^{d-1} + \dots + \\ f_{d-1}(a_1, \dots, a_n)(a_1x_1 + \dots + a_nx_n) + f_d(a_1, \dots, a_n) \\ \text{for all } a_1, \dots, a_n \in F \rangle, \end{aligned}$$

Pappacena proved in that paper that if $d = 2$ then this algebra is isomorphic to the Clifford algebra of a quadratic form, and therefore its structure is known.

In [Kuo11], Kuo studied the Clifford algebra of the polynomial $\Phi(z, a, b) = z^3 - eabz - f(a, b)$ and the results are very similar to the results Haile obtained in [Hai84]. The formulas for the simple images of the Clifford algebra are provided there only in case $f(a, b)$ is diagonal.

In Section 5, we study two cases separately, one of the polynomial $\Phi(z, a, b) = z^3 - rbz^2 - (eab + tb^2)z - (\alpha a^3 + \beta a^2b + \gamma ab^2 + \delta b^3)$ assuming that the characteristic of F is different from 3 and 2 and that it contains a primitive third root of unity, and of the polynomial $\Phi(z, a, b) = z^3 - eabz - f(a, b)$ assuming that the characteristic of F is 3. In particular we provide formulas for the images of the Clifford algebra studied in [Kuo11] in the non-diagonal case.

In Section 6 we present a further generalization of the algebra defined by Pappacena, the Clifford algebra of a degree d projective variety. The results from [HH07] are generalized for any 2-central variety whose defining equations are mutually diagonalizable quadratic equations.

Section 3 is based on a published paper, written collaboratively with my Ph.D advisor, Uzi Vishne. Section 5 is based on a collaborative work with Jung-Miao Kuo. Sections 2 and 6 are taken from a joint work with Daniel Krashen and Max Lieblich.

2. The Finite Linearization Problem

In this section we wish to prove the old conjecture that the Clifford algebra of any given form is finitely representable (see Remark 1.1).

Let d be a positive integer, F be an infinite field and $f(a_1, \dots, a_n) = \sum_{d_1+\dots+d_n=d} c_{d_1,\dots,d_n} a_1^{d_1} \dots a_n^{d_n}$ be a homogeneous form of degree d in n variables.

In this section we consider one of the two following cases:

- (1) The characteristic is prime to d .
- (2) d is prime and equal to the characteristic.

Let

$$C_f = F[x_1, \dots, x_n : (a_1x_1 + \dots + a_nx_n)^d = f(x_1, \dots, x_n) \forall a_1, \dots, a_n \in F]$$

be its Clifford algebra.

We say that f has a finite linearization if for some positive integer m , there exist matrices $X_1, \dots, X_n \in M_m(F)$ such that $(a_1X_1 + \dots + a_nX_n)^d = f(a_1, \dots, a_n)$ for all $a_1, \dots, a_n \in F$. It is clear that C_f is finitely representable if and only if f has a finite linearization.

The “Finite Linearization Problem” is the following question:

QUESTION 2.1. *Does f always have a finite linearization?*

This question originally arose in 1928 in Dirac’s treatment of the relativistic wave equation in quantum mechanics. He was mainly interested in the special case of $d = 2$ and $n = 4$.

It is important to note that given a finite field extension K/F , f has a finite linearization over F if and only if it has a finite linearization over K . Hence, in Case 1 we shall assume that F contains a primitive d th root of unity ρ .

In order to understand even the simplest examples in Case 1, one should be familiar with the concept of \mathbb{Z}_d -grading.

2.1. \mathbb{Z}_d -grading. Let \mathbb{Z}_d be the finite group with d elements obtained by taking the additive group of integers \mathbb{Z} modulo its subgroup $d\mathbb{Z}$.

An associative algebra A over F is \mathbb{Z}_d -graded if $A = A_0 \oplus \cdots \oplus A_{d-1}$ such that for every $a_j \in A_j$ and $a_k \in A_k$, $a_j a_k \in A_{j+k}$. The elements in A_j are called homogeneous elements of grade j .

EXAMPLE 2.2. *The matrix algebra $M_d(F)$ can be graded in such a way that each element $e_{k,k+j}$ is homogeneous of grade j .*

The \mathbb{Z}_d -graded tensor product of two \mathbb{Z}_d -graded algebras A and B is defined to be the algebra whose elements are sums of $a \otimes_{\mathbb{Z}_d} b$ such that $a \in A$ and $b \in B$, with addition that satisfies $(a + b) \otimes_{\mathbb{Z}_d} (c + d) = a \otimes_{\mathbb{Z}_d} c + a \otimes_{\mathbb{Z}_d} d + b \otimes_{\mathbb{Z}_d} c + b \otimes_{\mathbb{Z}_d} d$ and multiplication that satisfies $(a \otimes_{\mathbb{Z}_d} b_j) \cdot (a_k \otimes_{\mathbb{Z}_d} b) = \rho^{jk}(aa_k) \otimes_{\mathbb{Z}_d} (b_j b)$ for $b_j \in B_j$ and $a_k \in A_k$. In the special case of $d = 1$ we get the ordinary tensor product.

The theory of \mathbb{Z}_d -graded central simple algebras has been studied by many different mathematicians, such as Wall, Lam, Bahturin, Aljadeff and others (see [Lon74] or [KK12] for background). Here we shall recall only what we need. A \mathbb{Z}_d -graded central simple algebra is a unital associative algebra over a given field with no proper \mathbb{Z}_d -graded two-sided ideals. It is known that a central simple algebra that has a \mathbb{Z}_d -grading is a \mathbb{Z}_d -graded central simple algebra. Furthermore, a \mathbb{Z}_d -graded tensor product of \mathbb{Z}_d -graded central simple algebras is also a \mathbb{Z}_d -graded central simple algebra. Lastly, a \mathbb{Z}_d -graded central simple algebra over F always lives inside a finite matrix algebra over F , and therefore if C_f has an image which is a \mathbb{Z}_d -graded central simple algebra over F then it is finitely representable.

2.2. Formerly known results.

EXAMPLE 2.3. *Let us have a look at a given diagonal form $f = \alpha_1 u_1^d + \cdots + \alpha_n u_n^d$.*

In Case 1, for each $1 \leq k \leq n$, $F[\mu_k : \mu_k^d = \alpha_k]$ is \mathbb{Z}_d -graded with μ_k as the homogeneous element of grade 1. There is a \mathbb{Z}_d -graded representation $\Phi : C_f \rightarrow \otimes_{\mathbb{Z}_d} \prod_{k=1}^n F[\mu_k : \mu_k^d = \alpha_k]$, taking each x_k to μ_k .

In Case 2, we obtain a similar representation by replacing $\otimes_{\mathbb{Z}_d}$ with \otimes .

Consequently diagonal forms always have finite linearizations.

Childs proved in [Chi78] that if f is similar to a direct sum of unary and binary forms then f has a finite linearization.

Van den Bergh proved in [VdB87] that in the special case of $d = n = 3$, f has a finite linearization.

2.3. A positive answer in general. Let $g(a_1, \dots, a_n) = c_{d,0,\dots,0}a_1^d + \dots + c_{0,\dots,0,d}a_n^d$ be the diagonal part of f . For example, if $f(a_1, a_2) = c_{2,0}a_1^2 + c_{1,1}a_1a_2 + c_{0,2}a_2^2$ then $g(a_1, a_2) = c_{2,0}a_1^2 + c_{0,2}a_2^2$.

Let

$$C_g = F[y_1, \dots, y_n : (a_1y_1 + \dots + a_ny_n)^d = g(a_1, \dots, a_n) \forall a_1, \dots, a_n \in F]$$

be its Clifford algebra.

Let $\Phi_g : C_g \rightarrow B$ be a representation, taking each y_k to Y_k .

In Case 1 we assume that B is \mathbb{Z}_d -graded and that Y_k are all of grade 1. In Case 2 we do not impose any special assumptions on the representation.

For all n -tuples of non-negative integers satisfying $d_1 + \dots + d_n = d$, let c_{d_1,\dots,d_n} be the coefficient of $u_1^{d_1} \dots u_n^{d_n}$ in f , and let M_{d_1,\dots,d_n} be a copy of $M_d(F)$, graded as in Example 2.2.

In Case 1, we define a map $\Phi_f : C_f \rightarrow B \otimes_{\mathbb{Z}_d} \sum_{c_{d_1,\dots,d_n} \neq 0} M_{d_1,\dots,d_n}$, taking each x_k to $Y_k + \sum_{c_{d_1,\dots,d_n} \neq 0} x_{k;d_1,\dots,d_n}$. In Case 2 we define it in a similar way, just with \otimes instead of $\otimes_{\mathbb{Z}_d}$.

The element $x_{k;d_1,\dots,d_n}$ is defined as follows:

- If $d_k = 0$ then it is the zero matrix.
- If $d_k \neq 0$ and $d_1 = \dots = d_{k-1} = 0$ then it has c_{d_1,\dots,d_n} in the $(n, 1)$ entry, 1 in the entries $(1, 2), \dots, (d_k - 1, d_k)$, and 0 elsewhere.
- Otherwise, it has 1 in the entries $(d_1 + \dots + d_{k-1}, d_1 + \dots + d_{k-1} + 1), \dots, (d_1 + \dots + d_k - 1, d_1 + \dots + d_k)$ and 0 elsewhere.

For example, if $f(u_1, u_2) = \alpha u_1^3 + \beta u_1^2 u_2 + \gamma u_2^3$ then $x_{1;2,1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ \beta & 0 & 0 \end{pmatrix}$ and $x_{2;2,1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

THEOREM 2.4. Φ_f is a representation.

PROOF.

$$(a_1\Phi(x_1) + \dots + a_n\Phi(x_n))^d = ((a_1Y_1 + \dots + a_nY_n) + \sum_{c_{d_1,\dots,d_n} \neq 0} (a_1x_{1;d_1,\dots,d_n} + \dots + a_nx_{n;d_1,\dots,d_n}))^d.$$

In Case 1, because of the grading, we have $((a_1Y_1 + \dots + a_nY_n) + \sum_{c_{d_1,\dots,d_n} \neq 0} (a_1x_{1;d_1,\dots,d_n} + \dots + a_nx_{n;d_1,\dots,d_n}))^d = (a_1Y_1 + \dots + a_nY_n)^d + \sum_{c_{d_1,\dots,d_n} \neq 0} (a_1x_{1;d_1,\dots,d_n} + \dots + a_nx_{n;d_1,\dots,d_n})^d$.

In Case 2 we obtain the same equality because of the characteristic.

Finally, we have $(a_1Y_1 + \cdots + a_nY_n)^p = c_{d,0,\dots,0}a_1^d + \cdots + c_{0,\dots,0,d}a_n^d$, and $(a_1x_{1;d_1,\dots,d_n} + \cdots + a_nx_{n;d_1,\dots,d_n})^d = c_{d_1,\dots,d_n}a_1^{d_1} \cdots a_n^{d_n}$ and that completes the proof. \square

COROLLARY 2.5. *The form f always has a finite linearization.*

PROOF. From Example 2.3 it is clear that a finite linearization of g that satisfies the required conditions in Theorem 2.4 always exists. We obtain a finite linearization for f too using that theorem. \square

REMARK 2.6. *In Case 2, since the grading plays no role, one can similarly construct a finite linearization of the diagonal part of f for any given finite linearization of f .*

REMARK 2.7. *The representation Φ_f is not necessarily irreducible, even if Φ_g is.*

For example, let $f(a, b) = a^2 + 2ab + b^2$ and then $g(a, b) = a^2 + b^2$.

The Clifford algebra of g is $C_g = F[y_1, y_2 : y_1^2 = y_2^2 = 1, y_1y_2 = -y_2y_1] = M_2(F)$. This algebra is simple, and therefore is equal to all its homomorphic images. Φ_g can be the identity map on $M_2(F)$, having $Y_1 = y_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Y_2 = y_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The \mathbb{Z}_2 -grading of $M_2(F)$ can be according to the degrees of y_1 , i.e. the elements $e_{1,1}$ and $e_{2,2}$ are of grade 0 and $e_{1,2}$ and $e_{2,1}$ are of grade 1.

The obtained Φ_f will map C_f to $M_2(F) \otimes_{\mathbb{Z}_2} M_2(F)$ taking x_1 to $X_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes_{\mathbb{Z}_2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes_{\mathbb{Z}_2} \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$ and x_2 to $X_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes_{\mathbb{Z}_2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes_{\mathbb{Z}_2} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

The algebra C_f has only one two-sided ideal, the one generated by $x_1 - x_2$, and it has exactly two images, itself and itself modulo its ideal. Since $X_1 - X_2 \neq 0$, the image of Φ_f , $F[X_1, X_2]$ is isomorphic to C_f , and is in particular not irreducible, unlike the image of Φ_g which is isomorphic to C_g and therefore irreducible.

REMARK 2.8. *The rank of the obtained representation of C_f is not necessarily equal to the rank of the initial representation of C_g .*

For example, let $f(a, b) = ab$. Then $g(a, b) = 0$.

The base-field F is a representation of C_g of rank 1. The obtained representation of C_f will be $\Phi_f : C_f \rightarrow M_2(F)$ taking x_1 to $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

and x_2 to $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Φ_f is an isomorphism. Clearly the rank is 4, instead of 1.

This example holds regardless of characteristic.

CONJECTURE 2.9. *The obtained representation of C_f is of rank no less than the rank of the initial representation of C_g .*

REMARK 2.10. *The existence of a representation of C_g of rank r does not imply the existence of a representation of C_f of rank r , and vice versa.*

In Remark 2.8 we saw an example where C_g has a representation of rank 1, while C_f is simple of rank 4.

In the opposite direction, let us have a look again at the example given in Remark 2.7. There exists a homomorphism $\Phi_f : C_f \rightarrow F[\mu : \mu^2 = 1]$ taking x_1 and x_2 to μ . Here the representation is of rank 2 while C_g is simple of rank 4.

2.4. A note on higher dimensional representations. In [VdB87], Van den Bergh proved that binary forms of degree ≥ 4 have finite linearizations of unbounded high ranks.

In [CKM12], Emre, Kulkarni and Mustopa proved that ternary cubic forms have finite linearizations of unbounded high ranks.

However, these high rank finite linearizations are not easy to construct explicitly. Here we shall present an explicit example of a simple finite linearization of degree d^2 and index d for any $d \geq 4$ of any diagonal binary form of degree d :

EXAMPLE 2.11. *Let $f(a, b) = \alpha a^d + \beta b^d$ be a fixed binary form of degree d over F . Let $A = (\gamma, \delta)_{d,F} \otimes (\mu, \nu)_{d,F} = F[x, y] \otimes F[z, w]$, such that $\alpha = (-1)^{d-1}(\gamma\delta + \mu\nu\gamma)$ and $\beta = \delta + \nu\gamma$. Let $Y = y + wx$ and $X = yx + wzx$. By a straight-forward calculation $y(wx + yx + wzx) = \rho(wx + yx + wzx)y$, $yx(wx + wzx) = \rho(wx + wzx)yx$ and $(wx)(wzx) = \rho(wzx)(wx)$. Therefore for any $a, b \in F$, $(aX + bY)^d = b^d y^d + a^d (yx)^d + b^d (wx)^d + a^d (wzx)^d = a^d((-1)^{d-1}(\gamma\delta + \mu\nu\gamma)) + b^d(\delta + \nu\gamma) = \alpha a^d + \beta b^d$. The elements X and Y generate the algebra A over F .*

PROOF. $Z = YX - \rho XY = (\rho^{-1} - \rho)yxwx$. This element satisfies $yZ = \rho^2 Z y$ and $(wx)Z = \rho^{-1} Z (wx)$. Since $d \geq 4$, $\rho^{-1} \neq \rho^2$, and so by conjugating the element Y by Z we can show that $y, wx \in F[X, Y]$. Now, by conjugating the element X by wx we can show that $yx, wzx \in F[X, Y]$. The elements y, yx, wx, wzx generate the algebra A over F . \square

CONJECTURE 2.12. *We conjecture that the tensor product of cyclic algebras $A = \otimes_{k=1}^n (\alpha_k, \beta_k)_{d,F} = \otimes_{k=1}^n F[x_k, y_k]$ is generated by the elements $X = \sum_{k=1}^n x_1^{-1} \dots x_{k-1}^{-1} x_k y_1 \dots y_{k-1}$ and $Y = \sum_{k=1}^n x_1^{-1} \dots x_{k-1}^{-1} y_1 \dots y_k$. It is easy to see that X and Y span a d -central subspace of A , and therefore A would be a finite linearization of its exponentiation form. This way one could construct explicit finite linearizations of unbounded high ranks for any diagonal binary form. If $A = F[X, Y]$ and Conjecture 2.9 is true, then since this representation satisfies the conditions in Theorem 2.4, we can conclude that any form of degree greater or equal to four in at least two variables has finite linearizations of unbounded high ranks.*

3. The Clifford Algebra of a Short p -Central Space

Let d be an integer, and F be an infinite field of characteristic prime to d , containing a primitive d th root of unity ρ . Let A be a central simple algebra over F containing a d -central two-dimensional subspace $V = Fv + Fw$. The Clifford algebra of V is $C(V) = F[x, y : (ax + by)^d = (av + aw)^d \forall a, b \in F]$.

Let the underlying exponentiation form be $f(a, b) = \alpha_0 a^d + \alpha_1 a^{d-1} b + \dots + \alpha_d b^d$ for some coefficients $\alpha_0, \dots, \alpha_d \in F$.

According to Lemma 0.1, we can decompose $w = w_0 + w_1 + \dots + w_{d-1}$ such that $w_i v = \rho^i v w_i$ for any $0 \leq i \leq d-1$, and $w_0 = \frac{\alpha_1}{d\alpha_0} v$.

Similarly, inside the Clifford algebra, $y = y_0 + y_1 + \dots + y_{d-1}$ such that $y_i x = \rho^i x y_i$ for any $0 \leq i \leq d-1$, and $y_0 = \frac{\alpha_1}{d\alpha_0} x$.

There is a natural homomorphism from $C(V)$ to $F[V]$ taking x to v and y to w . This homomorphism also takes each y_i to v_i .

Replacing w by $w - \frac{\alpha_1}{d\alpha_0} v$, one can eliminate w_0 , and therefore we can always assume that $\alpha_1 = 0$ from the beginning.

DEFINITION 3.1. *Fixing the two basic elements v and w , including their order, we say that V is of type $T \subseteq \mathbb{Z}_d$ if $w_i = 0$ for every $i \notin T$. We call V short if T is of cardinality ≤ 2 .*

As we said before, $V = Fv + Fw$ is the image of the d -central subspace $V' = Fx + Fy$ of the Clifford algebra $C(V)$. Even if V is short of type $\{j, k\}$, it does not mean that V' is short.

EXAMPLE 3.2. *Let $V = Fv + Fw$ be a subspace of the 5-cyclic algebra $(\alpha, \beta)_{5,F} = F[v, w]$. Its Clifford algebra $C(V) = F[x, y]$ has the image $B = (\gamma, \delta) \otimes (\frac{\beta - \gamma - \delta}{\gamma}, \frac{\alpha}{\gamma\delta}) = F[q, r] \otimes F[s, t]$ taking x to qrt and y to*

$q + qs + r$. The image of V' in B is not short, and therefore V' is not short.

DEFINITION 3.3. We define the Clifford algebra of the short d -central space of type $\{j, k\}$ to be $C_{j,k}(V) = C(V) / \langle y_m : m \neq j, k \rangle$.

In [CV12] we proved that the following holds if $d = p$ is a prime.

THEOREM 3.4. (1) $C_{1,p-1}(V)$ is Azumaya.

(2) $Z(C_{1,p-1}(V)) = F[X, Y : Y(Y - \alpha_p) = \alpha_0 X^p + p^{-p} \alpha_2^p \alpha_0^{2-p}]$

(3) There is a one-to-one correspondence between the \bar{F} -rational points on this curve and the simple homomorphic images of $C_{1,p-1}(V)$. Every such image is either $(\alpha_p, \alpha_0)_{p,F}$ (the one corresponding to the point at infinity) or $(\alpha_0, t)_{p,K}$ where $K = F[s, t]$ and (s, t) is an \bar{F} -rational point with $t \neq 0$.

This generalizes the main result in [Hai84], since in the case of $p = 3$, $C(V) = C_{1,2}(V)$.

For the case of $p = 5$ we actually studied all possible kinds of short p -central spaces. There are essentially only two kinds, because a change of the p th root of unity sends $T = \{j, k\}$ to $\lambda T = \{\lambda j, \lambda k\}$ for some $\lambda \in \mathbb{Z}_d^\times$, so there is no real difference between the types $\{1, 4\}$ and $\{2, 3\}$, and similarly all the other types become $\{1, 3\}$.

We proved that if V is of type $\{1, 3\}$, then every simple homomorphic image of the Clifford algebra is a product of one or two cyclic division algebras of degree 5, whose center is some field extension of F . Explicit examples were given for both types of images.

In case that the exponentiation form is diagonal, we calculated all the simple images of $C_{1,3}(V)$ explicitly:

THEOREM 3.5. If $f(a, b) = \alpha a^5 + \beta b^5$ then any simple image A of $C_{1,3}(V)$ is one of the following:

(1) $A = (\alpha, \beta^2)_F$.

(2) $A = (\alpha, t)_K$ where $K = F(t, s)$ and $s^5 = \alpha^3 t^2 (\beta - t)$.

(3) $A = (\alpha, t)_{K \otimes_K (t', t'')_K}$ where $K = F(t, t', t'')$ and $t^3 + \alpha t' + \alpha^2 t'' = \beta t^2$.

(4) $A = (\alpha, t)_{K \otimes_K (t', t'')_K}$ where $K = F(t, t', t'', s)$, and $s^5 = \alpha^3 t t' t''^2 (\beta t^2 - t^3 - \alpha^2 t t' - \alpha t'')$.

This provides examples of an algebra of degree 25 and exponent 5 that is generated by a short 5-central space. In the following example we shall see how for any diagonal form of prime degree p there exists an algebra of degree p^2 and exponent p generated by a short p -central space whose exponentiation is equal to the given one:

EXAMPLE 3.6. Let $f(a, b) = \alpha a^p + \beta b^p$ be a diagonal form of degree p . Let $A = F[x, y] \otimes F[z, w]$. Let $X = w y x$, $Y = y + x^2 + z^2 y x$. Now, $(aX + bY)^p = (a w y x + b y + b x^2 + b z^2 y x)^p$. Since $(a w y x + b y + b z^2 y x)(b x^2) = \rho^2(b x^2)(a w y x + b y + b z^2 y x)$, $(b y)(a w y x + b z^2 y x) = \rho(a w y x + b z^2 y x)(b y)$ and $(a w y x)(b z^2 y x) = \rho^2(b z^2 y x)(a w y x)$, we have $(aX + bY)^p = a^p(a w y x)^p + b^p(y^p + (x^2)^p + (z^2 y x)^p) = a^p X^p + b^p Y^p$. It is easy to see that X and Y generate A .

4. The Clifford Algebra of a Short 4-Central Space

In this section we shall present some results concerning short d -central spaces when $d = 4$.

Let F be an infinite field of characteristic not 2, containing a primitive fourth root of unity i . Let $V = Fv + Fw$ be a 4-central subspace of some division algebra A . Let us assume that V is short of type $\{j, k\}$ for some $1 \leq j < k \leq 4$ (see Definition 3.1). Let $f(a, b) = \alpha_0 a^4 + \alpha_1 a^3 b + \alpha_2 a^2 b^2 + \alpha_3 a b^3 + \alpha_4 b^4$ be its underlying exponentiation form. We would like to study its Clifford algebra $C_{j,k}(V)$ (see Definition 3.3).

Assuming $\alpha_0 \neq 0$, by replacing w with $w - \frac{\alpha_1}{4\alpha_0}v$ we may assume that $\alpha_1 = 0$.

The Clifford algebra $C(V)$ is generated over F by x and y subject to the relations

$$(1) \quad x^4 = \alpha_0$$

$$(2) \quad x^3 * y = \alpha_1 = 0$$

$$(3) \quad x^2 * y^2 = \alpha_2$$

$$(4) \quad x * y^3 = \alpha_3$$

$$(5) \quad y^4 = \alpha_4$$

for some $\alpha_0, \dots, \alpha_4 \in F$.

Let us assume that $\alpha_0 \neq 0$.

As proven in Lemma 0.1, we can decompose $y = y_0 + y_1 + y_2 + y_3$ where $y_n x = i^n x y_n$ for $1 \leq n \leq 4$. However, $y_0 = \frac{\alpha_1}{d\alpha_0}x = 0$.

From $x^2 * y^2 = \alpha_2$ we obtain

$$(6) \quad x^2((2 + 2i)y_1 y_3 + (2 - 2i)y_3 y_1 + 2y_2^2) = \alpha_2$$

The algebra $C_{j,k}(V)$ is defined as in Definition 3.3.

For the case of $\{j, k\} = \{1, p-1\}$ we obtained a result similar to what we got for prime p .

THEOREM 4.1. *Assuming $\alpha_4 \neq \frac{\alpha_2^2}{8\alpha_0}$ and $\alpha_3 = 0$, if $\{j, k\} = \{1, 3\}$ then $C_{j,k}(V)$ is Azumaya whose center is a hyper-elliptic curve and every simple image of it is cyclic of degree 4. If $\{j, k\} = \{1, 3\}$ and $\alpha_3 \neq 0$ then $C_{j,k}(V) = 0$.*

PROOF. According to the definition of $C_{1,3}(V)$, $y_2 = 0$. Then Equation (6) becomes

$$(7) \quad x^2((2+2i)y_1y_3 + (2-2i)y_3y_1) = \alpha_2.$$

Relation (5) becomes, by conjugation by x , $\alpha_4 = y_1^4 + y_1^2 * y_3^2 + y_3^4$. Substituting Equation (7) in that relation leaves $\alpha_4 = y_1^4 + y_3^4 + \frac{\alpha_2^2}{8\alpha_0}$. Since the algebra is generated by x, y_1, y_3 , and y_1^4 commutes with those three, y_1^4 is central. A straightforward calculation shows that $w = (y_1y_3 + \frac{i\alpha_2}{4}x^{-2})x^{-1}$ commutes with the generators, and therefore is central too.

Let $K = F[y_1^4, w]$. Let us have a look at $C_f \otimes q(K)$. In this algebra, y_1 is invertible. Let $t_2 = -\frac{\alpha_2 i}{4}y_1^{-1}x^{-2}$ and $t_1 = y_3 - t_2$. Substituting $y_3 = t_1 + t_2$ in Equation (7) we get $y_1t_1 = it_1y_1$. From the relation $y_3x = -ixy_3$, by conjugation by y_1 we obtain $t_1x = -ixt_1$. Consequently, $t_1 \in q(K)y_1^{-1}x$, which means that $C_f \otimes q(K)$ is generated by x and y_1 over its center, and therefore $C_f \otimes q(K) = (\alpha_0, y_1^4)_{4,q(K)}$.

The center of C_f is the intersection of the center of $C_f \otimes q(K)$ and C_f , which is the ring generated over F by y_1^4 and w . Now, $\alpha_0 w^4 = (xw)^4 = y_1^8 + (\frac{\alpha_2^2}{8\alpha_0} - \alpha_4)y_1^4 + \frac{\alpha_4^2}{256\alpha_0^2}$. Setting $s = y_1^4$ and $r = w$, the center of C_f is the coordinate ring of the elliptic curve

$$(8) \quad s^2 + (\frac{\alpha_2^2}{8\alpha_0} - \alpha_4)s = \alpha_0 r^4 - \frac{\alpha_4^2}{256\alpha_0^2}.$$

Since $\alpha_4 \neq \frac{\alpha_2^2}{8\alpha_0}$, in every simple homomorphic image of C_f , either y_1 or y_3 is nonzero. Due to similar calculations as in the algebra $C_f \otimes q(K)$, every simple homomorphic image of C_f is a cyclic algebra of degree 4 over a field that is a quotient of $Z(C_f)$, and therefore is of the form $F[r_0, s_0]$ where (r_0, s_0) is an \bar{F} -rational point on the elliptic curve (8).

Let A be a simple homomorphic image of C_f , and let $s_0, r_0, \bar{x}, \bar{y}_1$ and \bar{y}_3 be the images of s, r, x, y_1 and y_3 respectively. Both s_0 and r_0 are in the center of A , which is a field, and therefore if they are nonzero then they are invertible. If $s_0 \neq 0$ then A is also an image of the algebra $C_f \otimes q(K)$, and then $A = (\bar{x}^4, \bar{y}_1^4)_{4,F[s_0, r_0]} = (\alpha_0, s_0)_{4,F[r_0, s_0]}$. Otherwise,

\bar{y}_3^4 must be nonzero. It is easy to see that A is generated by \bar{x} and \bar{y}_3 . If $\alpha_2 = 0$ then r_0 must be 0 too, and then $A = (\bar{y}_3^4, \bar{x}^4)_{4,F} = (\alpha_4, \alpha_0)_{4,F}$. If $\alpha_2 \neq 0$ then $(\frac{4\alpha_0}{\alpha_2}r_0)^4 = \alpha_0$, and so A is the 2×2 matrix algebra over either $F[\mu : \mu^4 = \alpha_0]$ (if α_0 has no fourth root in F) or over F (otherwise).

There is therefore a one-to-one correspondence between the \bar{F} -rational points on Curve (8) and the simple homomorphic images of C_f , that are all cyclic of degree 4, which means that C_f is Azumaya.

The last relation to take into consideration is Relation (4), which under these circumstances becomes $x*y_1^3 + x*y_1^2*y_3 + x*y_1*y_3^2 + x*y_3^3 = \alpha_3$. Taking only the part that commutes with x , we obtain $0 = \alpha_3$. The other parts become trivial by applying the other relations. \square

The two other possible types are $\{1, 2\}$ and $\{2, 3\}$. The latter can be obtained from the first by changing i to $-i$, and therefore they are essentially the same.

THEOREM 4.2. *If V is short of type $\{1, 2\}$ and its exponentiation form $f(a, b)$ is indecomposable then $C_{1,2}$ is a symbol algebra of degree 4 over a commutative ring over F . The explicit formulas are as follows:*

- (1) *If $\alpha_2 \neq 0$ and $\alpha_3 \neq 0$ then $C_{j,k}(V) = (\alpha_0, \frac{\alpha_3^2\alpha_2}{2\alpha_0})_{4,K} = K[\eta, \mu]$ where $K = F[\delta : \delta^4 = \frac{2\alpha_0^2\alpha_4}{\alpha_3^2\alpha_2} - \frac{2\alpha_0\alpha_2}{4\alpha_3^2} - \frac{\alpha_0}{16}]$. In this case, $V = F\eta + F(\mu + \mu\eta^{-1}\delta + \frac{\alpha_3^2}{4}\mu^{-2}\eta^{-1})$.*
- (2) *If $\alpha_2 \neq 0$, $\alpha_3 = 0$ and $\alpha_4 \neq \frac{\alpha_2^2}{4\alpha_0}$ then $C_{j,k}(V) = (\alpha_0, \alpha_4 - \frac{\alpha_2^2}{4\alpha_0})_{4,K}$ where $K = F[\mu, \nu : \mu^2 = 0, \nu^2 = \frac{\alpha_2}{2\alpha_0}(\alpha_4 - \frac{\alpha_2^2}{4\alpha_0}), \mu\nu = \nu\mu]$*
- (3) *If $\alpha_2 = 0$, $\alpha_3 \neq 0$ and $\alpha_4 \neq 0$ then $C_{j,k}(V) = (\alpha_0, \alpha_4)_{4,K}$ where $K = F[\mu : \mu^2 = 0]$.*
- (4) *If $\alpha_2 = \alpha_3 = 0$ and $\alpha_4 \neq 0$ then $C_{j,k}(V) = (\alpha_0, \alpha_4)_{4,K}$ where $K = F[\mu, \nu : \mu^2 = \nu^2 = \mu\nu - \nu\mu = 0]$.*

PROOF. The type is $\{1, 2\}$, which means that $y = y_1 + y_2$. Therefore, Equation (6) becomes $x^2(2y_2^2) = \alpha_2$, which means that $y_2^2 = \frac{\alpha_2}{2}x^{-2}$.

Assume $\alpha_2 \neq 0$. Then $y_2^2y_1 + y_1y_2^2 = 0$, and therefore $y_1 = t_1 + t_3$ such that $t_k y_2 = i^k y_2 t_k$.

From Relation (4) we obtain (by conjugation by x)

$$(9) \quad x * y_1^2 * y_2 = \alpha_3$$

and

$$(10) \quad x * y_1 * y_2^2 = 0.$$

From the Equation (9) we obtain

$$(11) \quad (1+i)xy_1^2y_2 + 2xy_1y_2y_1 + (1-i)xy_2y_1^2 = \alpha_3$$

and from the Equation (10) we obtain

$$(12) \quad (1+i)xy_1y_2^2 + (1+(-1)+1+i)xy_2^2y_1 = 0.$$

Equation (12) is trivial. From Equation (11) we obtain

$$(13) \quad (2i+2)t_1t_3 + (2-2i)t_3t_1 - 4it_3^2 = \alpha_3y_2^{-1}x^{-1}.$$

By conjugation by y_2 we obtain the following two relations:

$$(14) \quad (2i+2)t_1t_3 + (2-2i)t_3t_1 = 0,$$

$$(15) \quad -4it_3^2 = \alpha_3y_2^{-1}x^{-1}.$$

From Equation (14) we obtain $t_1t_3 = it_3t_1$.

From Equation (15) we obtain $t_3^2 = \frac{\alpha_3i}{4}y_2^{-1}x^{-1}$.

Assume $\alpha_3 \neq 0$. Then $y_2 = \frac{\alpha_3i}{4}t_3^{-2}x^{-1}$.

Now, $\alpha_4 = (y_1 + y_2)^4$. By conjugation by x , $(y_1 + y_2)^4 = y_1^4 + y_2^4$, and since $t_1t_3 = it_3t_1$, $y_1^4 = t_1^4 + t_3^4$. Hence $\alpha_4 = t_1^4 + \frac{\alpha_3^2\alpha_2}{32} + \frac{\alpha_2^2}{4\alpha_0}$, which means that $t_1^4 = \alpha_4 - \frac{\alpha_3^2\alpha_2}{32} - \frac{\alpha_2^2}{4\alpha_0}$.

Setting $\eta = x$, $\mu = t_3$ and $\delta = xt_3^{-1}t_1$, we have $K = F[\delta]$ as the center of $C_{1,2}(V)$. $C_{1,2}(V) = F[\eta, \mu] \otimes K = (\alpha_0, \frac{\alpha_3^2\alpha_2}{2})_{4,F} \otimes K$. $V = Fx + Fy = Fx + F(y_1 + y_2) = Fx + F(t_3 + t_1 + y_2) = F\eta + F(\mu + \mu\eta^{-1}\delta + \frac{\alpha_3i}{4}\mu^{-2}\eta^{-1})$.

Assume $\alpha_2 \neq 0$ and $\alpha_3 = 0$. Then $t_3^2 = 0$. Consequently $t_1^4 = \alpha_4 - \frac{\alpha_2^2}{4\alpha_0}$. Assume $\alpha_4 - \frac{\alpha_2^2}{4\alpha_0} \neq 0$. Setting $\eta = x$, $\mu = t_1$, $\gamma = x^{-1}t_3t_1^{-1}$ and $\delta = x^{-1}t_1^2y_2$ we have $K = F[\gamma, \delta]$ as the center of $C_{1,2}(V)$. $C_{1,2}(V) = F[\eta, \mu] \otimes K = (\alpha_0, \alpha_4 - \frac{\alpha_2^2}{4\alpha_0})_{4,F}$.

If $\alpha_4 = \frac{\alpha_2^2}{4\alpha_0}$ then $t_1^4 = 0$. Therefore $f(u, v) = \alpha_0u^4 + \alpha_2u^2v^2 + \frac{\alpha_2^2}{4\alpha_0}v^4 = \alpha_0(u^2 + \frac{\alpha_2}{2\alpha_0}v^2)^2$. In this case $f(a, b)$ is decomposable, contradictory to the assumption.

If $\alpha_2 = 0$ then we cannot decompose y_1 to $t_1 + t_3$ by conjugation by y_2 because y_2 is not invertible. However, from $(1+i)y_1^2y_2 + 2y_1y_2y_1 + (1-i)y_2y_1^2 = \alpha_3x^{-1}$ we obtain $y_2 = t_1 + t_2 + t_3$ where $t_3 = \frac{\alpha_3i}{4}y_1^{-2}x^{-1}$ and $y_1t_k = i^k t_k y_1$.

We have $\alpha_4 = y_1^4 + y_2^4 = y_1^4$. Assume that $\alpha_4 \neq 0$. Now, $y_2^2 = 0 = t_1^2 + t_2^2 + t_3^2 + t_1t_2 + t_2t_1 + t_1t_3 + t_3t_1 + t_2t_3 + t_3t_2 = t_1^2 + t_2^2 + t_3^2 + t_1t_2 + t_2t_1 + 2t_1t_3$. By conjugation by y_1 , $t_1^2 + t_3^2 = 0$, $t_1t_2 + t_2t_1 = 0$ and $t_2^2 + 2t_1t_3 = 0$.

Assume $\alpha_0 \neq 0$ and so $t_1 \in F[t_2, x, y_1]$. $K = F[x^2 y_1^2 t_2]$ is the center of $C_{1,2}(V)$. $C_{1,2}(V) = (\alpha_0, \alpha_4)_K$.

If $\alpha_3 = 0$ then $t_1^2 = t_2^2 = t_1 t_2 - t_2 t_1 = 0$. $K = F[x^2 y_1^2 t_2, x^{-1} y_1^2 t_1]$ is the center of $C_{1,2}(V)$. $C_{1,2}(V) = (\alpha_0, \alpha_4)_{4,K}$. \square

REMARK 4.3. If $\alpha_2 \neq 0$, $\alpha_3 = 0$ and $\alpha_4 = \frac{\alpha_2^2}{4\alpha_0}$ then $f(u, v) = \alpha_0 u^4 + \alpha_2 u^2 v^2 + \frac{\alpha_2^2}{4\alpha_0} v^4 = \alpha_0 (u^2 + \frac{\alpha_2}{2\alpha_0} v^2)^2$. In this case $C_{j,k}(V)/\langle t_1, t_3 \rangle = F[x, y_2] = (\mu, \frac{\alpha_2}{2} \mu^{-1})_{2,K}$ where $K = F[\mu : \mu^2 = \alpha_0]$. This means that $\text{Rad}(C_{j,k}(V)) = \langle t_1, t_3 \rangle$.

5. The Clifford Algebra of a Monic Polynomial

This section is based on a joint work with Jung-Miao Kuo.

In [Pap00], Pappacena generalized the notion of the Clifford algebra to the algebra associated to a monic polynomial (with respect to the first variable) $\Phi(z, a_1, \dots, a_n) = z^d - \sum_{k=1}^d f_k(a_1, \dots, a_n) z^{d-k}$, where each f_k is a homogeneous form of degree k . This algebra, denoted there by C_Φ , is defined to be

$$\begin{aligned} F\langle x_1, \dots, x_n : (a_1 x_1 + \dots + a_n x_n)^d \\ = f_1(a_1, \dots, a_n)(a_1 x_1 + \dots + a_n x_n)^{d-1} + \dots + \\ f_{d-1}(a_1, \dots, a_n)(a_1 x_1 + \dots + a_n x_n) + f_d(a_1, \dots, a_n) \\ \text{for all } a_1, \dots, a_n \in F \rangle, \end{aligned}$$

Pappacena proved in that paper that if $d = 2$ then this algebra is isomorphic to the Clifford algebra of a quadratic form, and therefore its structure is known.

In [Kuo11], Kuo studied the Clifford algebra of the polynomial $\Phi(z, a, b) = z^3 - eabz - f(a, b)$ and the results are very similar to the results Haile obtained in [Hai84]. The formulas for the simple images of the Clifford algebra are provided there only in case $f(a, b)$ is diagonal.

In this section we study the Clifford algebra of the monic polynomial $\Phi(z, a, b) = z^3 - f_1(a, b)z^2 - f_2(a, b)z - f_3(a, b)$ in two distinct cases:

- (1) $\text{char}(F) \neq 2, 3$, $f_1(a, 0) = f_2(a, 0) = 0$.
- (2) $\text{char}(F) = 3$, $f_1(a, b) = 0$ and $f_2(a, b) = eab$.

5.1. Case 1. Let $\Phi(z, a, b) = z^3 - rbz^2 - (eab + tb^2)z - (\alpha a^3 + \beta a^2 b + \gamma ab^2 + \delta b^3)$ where $r, t, e, \alpha, \delta, \beta, \gamma \in F$.

The algebra C_Φ is by definition

$$\begin{aligned} C_\Phi &= F\langle x, y: x^3 = \alpha, \\ &\quad x^2 * y = rx^2 + ex + \beta, \\ &\quad x * y^2 = rxy + ryx + tx + ey + \gamma, \\ &\quad y^3 = ry^2 + ty + \delta \rangle. \end{aligned}$$

We assume that $\alpha \neq 0$ and F contains a primitive third root of unity ρ . According to Lemma 0.1, since $x^3 \in F^\times$, there exist $y_0, y_1, y_2 \in C_\Phi$ such that

$$(16) \quad y = y_0 + y_1 + y_2 \quad \text{and} \quad y_i x = \rho^i x y_i.$$

In this case, we say that y_i ρ^i -commutes with x . Under this decomposition, the relation $x^2 * y = rx^2 + ex + \beta$ is equivalent to $y_0 = (3\alpha)^{-1}(ex^2 + \beta x + \alpha r)$. Substituting this in the relation $x * y^2 = rxy + ryx + tx + ey + \gamma$, we obtain by a straight-forward calculation that

$$(17) \quad y_1 y_2 = \rho y_2 y_1 + \frac{(1-\rho)D_1}{3\alpha} x^2 - \frac{(1-\rho)D_2}{9\alpha}$$

where

$$D_1 = \gamma + \frac{er}{3} - \frac{\beta^2}{3\alpha} \quad \text{and} \quad D_2 = e\beta - 3\alpha t - \alpha r^2.$$

Let

$$w = x^{-1} y_2 y_1 + \rho^2 \frac{D_1}{3\alpha} x + \frac{D_2}{9\alpha} x^{-1}.$$

LEMMA 5.1. *The elements w, y_1^3 and y_2^3 are in the center of C_Φ .*

PROOF. Clearly, w commutes with x . By Equation (17) we see that $y_i w = w y_i$, $i = 1, 2$. Thus, w commutes with y and hence is central in C_Φ . Similarly, one can check that y_1^3 and y_2^3 are central in C_Φ . \square

The relation $y^3 = ry^2 + ty + \delta$ may be split into three parts due to conjugation by x . The part on the left-hand side which ρ -commutes with x is $y_0^2 * y_1 + y_1^2 * y_2 + y_2^2 * y_0$ and on the right-hand side it is $ry_0 * y_1 + ry_2^2 + ty_1$. A direct computation shows that $y_0^2 * y_1 = (3\alpha)^{-1}e\beta y_1 + 3^{-1}r^2 y_1 - (3\alpha)^{-1}\rho e r x^2 y_1 - (3\alpha)^{-1}\rho^2 \beta r x y_1$, $y_1^2 * y_2 = -(3\alpha)^{-1}D_2 y_1$, $y_2^2 * y_0 = r y_2^2$ and $r y_0 * y_1 = 3^{-1}2r^2 y_1 - (3\alpha)^{-1}\rho e r x^2 y_1 - (3\alpha)^{-1}\rho^2 \beta r x y_1$. Thus, $y_0^2 * y_1 + y_1^2 * y_2 + y_2^2 * y_0$ is equal to $r y_0 * y_1 + r y_2^2 + t y_1$. Similarly, the part on the left-hand side which ρ^2 -commutes with x is equal to that on the right-hand side: $y_0^2 * y_1 + y_1^2 * y_2 + y_2^2 * y_0 = r y_0 * y_2 + r y_1^2 + t y_2$.

So let us consider the parts on both sides which commute with x :

$$(18) \quad \left(\frac{1}{3\alpha}(ex^2 + \beta x + \alpha r) \right)^3 + y_1^3 + y_2^3 + \frac{1}{3\alpha}(ex^2 + \beta x + \alpha r) * y_1 * y_2 = \\ ry_0^2 + ry_1 * y_2 + ty_0 + \delta.$$

We first compute

$$\begin{aligned} & (ex^2 + \beta x) * y_1 * y_2 \\ &= e((2 + \rho^2)x^2 y_1 y_2 + (2 + \rho)x^2 y_2 y_1) + \beta((2 + \rho)xy_1 y_2 + (2 + \rho^2)xy_2 y_1) \\ &= e \left(-3\rho^2 x^2 y_2 y_1 - \rho D_1 x + \frac{\rho D_2}{3\alpha} x^2 \right) + \beta \left(D_1 - \frac{D_2}{3\alpha} x \right) \\ &= e \left(-3\rho^2 \alpha w - \frac{D_2}{3\alpha} x^2 \right) + \beta \left(D_1 - \frac{D_2}{3\alpha} x \right) \end{aligned}$$

where the second equality holds by applying Equation (17). Substituting this in Equation (18) we then obtain by another straight-forward calculation that

$$(19) \quad D + y_1^3 + y_2^3 - \rho^2 ew = 0,$$

where

$$D = \frac{e^3}{27\alpha} + \frac{\beta^3}{27\alpha^2} - \frac{2r^3}{27} + \frac{\beta}{3\alpha} D_1 - \frac{rt}{3} - \delta.$$

Consequently, via the decomposition in (16) with y_0 taken as $(3\alpha)^{-1}(ex^2 + \beta x + \alpha r)$, C_Φ is an F -algebra generated by x, y_1, y_2 subject to the relations $x^3 = \alpha$, $y_i x = \rho^i x y_i$ and Equations (17), (19). Thus we have the following result.

LEMMA 5.2. *As an $F[y_1^3, w]$ -module, C_Φ is finitely generated by the 27 elements $x^i y_1^j y_2^k$, where $0 \leq i, j, k \leq 2$.*

Let us consider the algebra after the localization $C_\Phi[y_1^{-3}]$. Since in this algebra y_1 is invertible, from the choice of w , we have

$$(20) \quad y_2 = xy_1^{-1}w - \rho^2 \frac{D_1}{3\alpha} x^2 y_1^{-1} - \frac{D_2}{9\alpha} y_1^{-1},$$

and so

$$y_2^3 = \alpha y_1^{-3} w^3 - \frac{D_1^3}{27\alpha} y_1^{-3} - \frac{D_2^3}{729\alpha^3} y_1^{-3} - \rho^2 \frac{D_1 D_2}{9\alpha} w y_1^{-3}.$$

Therefore, substituting this in Equation (19) we get

$$D + y_1^3 + \alpha y_1^{-3} w^3 - \frac{D_1^3}{27\alpha} y_1^{-3} - \frac{D_2^3}{729\alpha^3} y_1^{-3} - \rho^2 \frac{D_1 D_2}{9\alpha} w y_1^{-3} - \rho^2 ew = 0.$$

Consequently,

$$(21) \quad (D - \rho^2 ew)y_1^3 + y_1^6 + \alpha w^3 - \frac{D_1^3}{27\alpha} - \frac{D_2^3}{729\alpha^3} - \rho^2 \frac{D_1 D_2}{9\alpha} w = 0.$$

The last equality also holds in C_Φ .

We next show that the center Z of C_Φ is $F[y_1^3, w]$ and it is isomorphic to the coordinate ring of the affine elliptic curve

$$(22) \quad E: (D - \rho^2 eR)S + S^2 + \alpha R^3 - \frac{D_1^3}{27\alpha} - \frac{D_2^3}{729\alpha^3} - \rho^2 \frac{D_1 D_2}{9\alpha} R = 0,$$

where the discriminant is assumed to be nonzero. Let E also denote the elliptic curve with affine piece given by Equation (22).

PROPOSITION 5.3. *There is an F -algebra isomorphism from $C_\Phi[y_1^{-3}]$ into the symbol algebra $(\alpha, S)_{3, F(E)}$ over the function field $F(E)$ of the elliptic curve E .*

PROOF. Let u, v be the generators of $(\alpha, S)_{3, F(E)}$ satisfying $u^3 = \alpha, v^3 = S$ and $vu = \rho uv$. Let ϕ be the F -algebra homomorphism from C_Φ into $(\alpha, S)_{3, F(E)}$ defined as follows

$$\begin{aligned} \phi: C_\Phi &\rightarrow (\alpha, S)_{3, F(E)} \\ x &\mapsto u \\ y_1 &\mapsto v \\ y_2 &\mapsto u \left(R - \rho^2 \frac{D_1}{3\alpha} u - \frac{D_2}{9\alpha} u^{-1} \right) v^{-1}. \end{aligned}$$

One can check that $x^3 = \alpha, y_i x = \rho^i x y_i$ and the relations in Equations (17) and (19) are preserved under the map ϕ . Thus it is well-defined and $\phi(w) = R$. Furthermore, it induces a homomorphism from $C_\Phi[y_1^{-3}]$ to $(\alpha, S)_{3, F(E)}$, which we also denote by ϕ .

Notice that from Equations (20) and (21), $C_\Phi[y_1^{-3}]$ as an $F[y_1^{\pm 3}]$ -module is finitely generated by the 27 elements $x^i y_1^j w^k$, where $0 \leq i, j, k \leq 2$. Since the images of these elements are linearly independent over $F[S^{\pm 1}]$ and ϕ when restricted to $F[y_1^{\pm 3}]$ is injective, it follows that ϕ itself is injective. \square

COROLLARY 5.4. *The center Z of C_Φ is $F[y_1^3, w]$ and it is isomorphic to the coordinate ring $F[E]$ of the affine elliptic curve E .*

PROOF. By Proposition 2.1, $F[y_1^3, w] \cong F[E]$, a Dedekind domain. Furthermore, we see from its proof that $\phi(C_\Phi)F(E) = (\alpha, S)_{3, F(E)}$. In particular, the center of $\phi(C_\Phi)$ is contained in $F(E)$. Therefore

$F[E] = \phi(F[y_1^3, w]) \subseteq \phi(Z) \subseteq F(E)$. It follows from Lemma 5.2 and the injectivity of ϕ that $Z = F[y_1^3, w] \cong F[E]$. \square

Now the center of $C_\Phi[y_1^{-3}]$ is $Z_{(y_1^3)} = F[y_1^{\pm 3}, w] \cong F[E]_{(S)}$ in which y_1^3 is invertible. Thus we have the following result.

COROLLARY 5.5. *$C_\Phi[y_1^{-3}]$ is the symbol Azumaya algebra $(\alpha, y_1^3)_{3, F[y_1^{\pm 3}, w]}$. Similarly, $C_\Phi[y_2^{-3}] = (y_2^3, \alpha)_{3, F[y_2^{\pm 3}, w]}$.*

From now on, we restrict ourselves to the following conditions: $D \neq 0$ and the subalgebra $F[x : x^3 = \alpha]$ is a field.

PROPOSITION 5.6. *In every homomorphic image of C_Φ , either $y_1^3 \neq 0$ or $y_2^3 \neq 0$. In particular, if the image is simple then either y_1^3 or y_2^3 is invertible.*

PROOF. Assume to the contrary that $y_1^3 = y_2^3 = 0$. Then by Equation (19), $D = \rho^2 ew$. If $e = 0$, then $D = 0$, a contradiction. If $e \neq 0$, then by the choice of w , we have that $y_2 y_1 = \rho e^{-1} D x - (3\alpha)^{-1} \rho^2 D_1 x^2 - (9\alpha)^{-1} D_2$, which is invertible as a nonzero element of the field $F[x]$. However this means that y_1 is invertible too, which is a contradiction. \square

COROLLARY 5.7. *The algebra C_Φ is Azumaya of rank 9.*

PROOF. By Corollary 5.4 and Lemma 5.2, C_Φ is finitely generated as a module over its center $Z = F[y_1^3, w]$. For every maximal ideal m of Z , it follows from Proposition 5.6 and Corollary 5.5 that C_Φ/mC_Φ is a central simple algebra of degree 3 over the field Z/m . Therefore, C_Φ is Azumaya of rank 9. \square

REMARK 5.8. *Another way to prove that C_Φ is Azumaya is the following: Every $\Phi(Z, X, Y) = Z^3 - \sum_{k=1}^3 f_k(X, Y)Z^{3-k}$ can be linearly transformed over \bar{F} into the one with $f_1 = 0$, $f_2 = eXY$ and $f_3 = X^3 + Y^3$ for some $e \in \bar{F}$ (in characteristic not 2 or 3), and therefore that C_Φ is Azumaya follows immediately from [Kuo11] and the fact that the construction of C_Φ is functorial in F .*

We are finally able to describe explicitly the simple homomorphic images of C_Φ .

THEOREM 5.9. *There is a one-to-one correspondence between the simple homomorphic images of C_Φ and the Galois orbits of \bar{F} -rational points on the affine elliptic curve E as follows: the Galois orbit containing (R_0, S_0) on E gives rise to the $F(R_0, S_0)$ -central simple algebra $(\alpha, S_0)_{3, F(R_0, S_0)}$ if $S_0 \neq 0$ and $(\rho^2 e R_0 - D, \alpha)_{3, F(R_0, S_0)}$ if $S_0 = 0$.*

PROOF. Since C_Φ is Azumaya, there is a one-to-one correspondence between its simple homomorphic images and maximal ideals of its center $Z \cong F[E]$. Furthermore, y_1^3, w in the center correspond to S, R . Thus by Equation (19), y_2^3 corresponds to $\rho^2 eR - S - D$. Therefore, the result follows from Proposition 5.6 and Corollary 5.5. \square

Define the function Ψ from the group $E(F)$ of F -rational points on the elliptic curve E into the Brauer group of F as follows

$$\begin{aligned} \Psi: E(F) &\rightarrow Br(F) \\ (R_0, S_0) &\mapsto \begin{cases} [(\alpha, S_0)_{3,F}] & \text{if } S_0 \neq 0 \\ [(\rho^2 eR_0 - D, \alpha)_{3,F}] & \text{if } S_0 = 0 \end{cases} \\ O &\mapsto 1. \end{aligned}$$

We next show that the arguments used in [Kuo11, Section 4] can be applied here to show that Ψ is a group homomorphism.

PROPOSITION 5.10. *The function Ψ is a group homomorphism.*

PROOF. Identify $Z = F[y_1^3, w]$ with $F[E]$. Similar to the proof of [Kuo11, Corollary 4.3], the Brauer class of C_Φ in $Br(F(E))$ is unramified everywhere. Thus, the algebra C_Φ can be extended to a Brauer class in $Br(E)$. Also, $C_\Phi \otimes_{F[E]} F(E) = (\alpha, S)_{3,F(E)} = (\alpha, T)_{3,F(E)}$, where $T = R^3/S^2$. By Equation (22) we see that

$$(23) \quad T = \frac{D - \rho^2 eR}{-\alpha S} - \frac{1}{\alpha} + \frac{D_1^3}{27\alpha^2 S^2} + \frac{D_2^3}{729\alpha^4 S^2} + \frac{\rho^2 D_1 D_2 R}{9\alpha^2 S^2}.$$

Let ν be the discrete valuation on $F(E)$ corresponding to O . Then $\nu(R) = -1$ and $\nu(S) = -3/2$. Thus $\nu(T) = 0 = \nu(\alpha)$, and hence the specialization of $C_\Phi \otimes_{F[E_a]} F(E)$ at O is $(\alpha, \bar{T})_{3,F}$ where \bar{T} is the image of T in the residue field of O . By Equation (23), $\bar{T} = -1/\alpha = N_{F(\sqrt[3]{\alpha})/F}((-1/\alpha)\sqrt[3]{\alpha^2})$. Thus, the specialization at O of the class of C_Φ in $Br(E)$ is trivial. Therefore, similar to the proof of [Kuo11, Theorem 4.1], the result now follows from Lemma 3.2 and Theorem 3.5 of [CK12]. \square

Since C_Φ is Azumaya of rank 9, one can check that the homogeneous polynomial $\Phi(X, Y, Z)$ over F is then absolutely irreducible. Let C denote the cubic curve given by the equation $\Phi(X, Y, Z) = 0$. The computations in [ARVT05] show that the elliptic curve E is the Jacobian of the cubic curve C . We have the following two analogues of Proposition 4.5 and Theorem 4.6 of [Kuo11] with similar proofs, which we therefore skip.

PROPOSITION 5.11. *The group homomorphism $\Psi: E(F) \rightarrow Br(F)$ maps onto the relative Brauer group $Br(F(C)/F)$.*

PROPOSITION 5.12. *The Azumaya algebra C_Φ is split if and only if the cubic curve C has an F -rational point.*

5.2. Case 2. Let $\Phi(z, a, b) = z^3 - eabz - (\alpha a^3 + \beta a^2b + \gamma ab^2 + \delta b^3)$ for some $e, \alpha, \delta, \beta, \gamma \in F$, $\text{char}(F) = 3$ and $\alpha \neq 0$.

C_Φ is by definition

$$\begin{aligned} F\langle x, y: x^3 &= \alpha, \\ y^3 &= \delta, \\ x^2 * y &= ex + \beta, \\ x * y^2 &= ey + \gamma \rangle. \end{aligned}$$

We treat the two cases of $e = 0$ and $e \neq 0$ separately.

5.2.1. $e = 0$. In this case, C_Φ is simply the ordinary Clifford algebra of the form $f(X, Y) = \alpha X^3 + \beta X^2Y + \gamma XY^2 + \delta Y^3$. The element x is 3-central. Therefore, according to Lemma 0.3, we can decompose y as

$$y = y_2 - y_1$$

such that

$$(24) \quad xy_2 - y_2x = y_1, xy_1 - y_1x = y_0, \text{ where } y_0x = xy_0.$$

Substituting this in the relation $x^2 * y = \beta$, by a straight-forward calculation we get $y_0 = \beta$. Thus from the relation $x * y^2 = \gamma$, we then get

$$(25) \quad y_1y_2 - y_2y_1 = \gamma.$$

Substituting this further in $y^3 = \delta$ leaves

$$(26) \quad y_2^3 - y_1^3 = \delta.$$

Therefore, C_Φ is an F -algebra generated by x, y_1, y_2 subject to the relations $x^3 = \alpha$, Equation (24), where $y_0 = \beta$, and Equations (25), (26). We shall see in particular that, unless f is diagonal, C_Φ is Azumaya.

Let $w = \beta y_2 + \gamma x + y_1^2$. It is a straight-forward calculation to see that w, y_1^3 and y_2^3 commute with x, y_1 and y_2 , and therefore they are central in C_Φ . Consider the following affine curve

$$E_\Delta: s^2 = r^3 + \Delta,$$

where $\Delta = -\gamma^3\alpha + \gamma^2\beta^2 - \beta^3\delta + \beta^6$. We next show that in the case of $\beta \neq 0$, C_Φ is Azumaya of rank 9 and its center is isomorphic to the coordinate ring of E_Δ .

LEMMA 5.13. *If $\beta \neq 0$ then the subalgebra $F[w, y_1^3]$ of the center of C_Φ is isomorphic to the coordinate ring $F[r, s]$ of the affine curve E_Δ . In particular it is an integral domain.*

PROOF. If $\beta \neq 0$, then $y_2 = \beta^{-1}(w - \gamma x - y_1^2)$ and substituting it in Equation (26) yields $\beta^{-3}(w^3 - \gamma^3 \alpha - y_1^6 + \gamma^2 \beta^2) - y_1^3 = \delta$, or equivalently,

$$w^3 + \Delta = (y_1^3 - \beta^3)^2.$$

Consequently $F[w, y_1^3]$ is the F -subalgebra generated by w and y_1^3 subject only to the relation in the equation above. Thus the map defined by sending r, s to $w, y_1^3 - \beta^3$ clearly gives an F -algebra isomorphism. \square

Note that E_Δ is smooth (and then an affine elliptic curve) if and only if its discriminant is nonzero or $\Delta \neq 0$. In this case, its coordinate ring is a Dedekind domain. In the following, for any integral domain R , $q(R)$ stands for its quotient field.

THEOREM 5.14. *If $\beta \neq 0$ then*

- (1) C_Φ is Azumaya of rank 9.
- (2) *The center of C_Φ is the subalgebra $F[w, y_1^3]$, and it is isomorphic to the coordinate ring of E_Δ .*
- (3) *There is a one-to-one correspondence between the Galois orbits of \bar{F} -rational points on E_Δ and the simple homomorphic images of C_Φ , taking each Galois orbit containing (r_0, s_0) to the degree 3 cyclic algebra $[\alpha\beta^{-3}(s_0 + \beta^3), \alpha]_{3, F[r_0, s_0]}$.*

PROOF. In this case, $y_2 = \beta^{-1}(w - \gamma x - y_1^2)$. Let $z = \beta^{-1}xy_1$. It is a straight-forward calculation to see that $xz - zx = x$ and $z^3 - z = \alpha\beta^{-3}y_1^3$. Consequently, in $C_\Phi \otimes_{F[w, y_1^3]} q(F[w, y_1^3])$, x and z generate over $q(F[w, y_1^3])$ a cyclic algebra of degree 3 in which x is 3-central and z is Artin-Schreier. The subalgebra $q(F[w, y_1^3])[x, z]$ in fact contains all the generators of C_Φ , and therefore $q(F[w, y_1^3])[x, z] = C_\Phi \otimes q(F[w, y_1^3])$. In particular, the center of $C_\Phi \otimes q(F[w, y_1^3])$ is $q(F[w, y_1^3])$, and hence the center of C_Φ is $F[w, y_1^3]$, which is isomorphic to the coordinate ring $F[r, s]$ of the affine curve E_Δ by the Lemma above. Identifying $F[w, y_1^3]$ with $F[r, s]$, we have $r = w$ and $s = y_1^3 - \beta^3$.

Let there be a simple homomorphic image A of C_Φ . Let r_0, s_0, x' and y'_1 be the images in A of r, s, x and y_1 , respectively. In particular $x'^3 = \alpha$ and $y'^3_1 = s_0 + \beta^3$. Furthermore, A is generated by x' and $z' = \beta^{-1}x'y'_1$ over $F[r_0, s_0]$, where $z'^3 - z' = \alpha\beta^{-3}(s_0 + \beta^3)$. These two elements satisfy $x'z' - z'x' = x'$, and therefore A is a cyclic algebra of degree 3 over $F[r_0, s_0]$ in which x' is 3-central and z' is Artin-Schreier. Hence A has the symbol presentation $[z'^3 - z', x'^3]_{3, F[r_0, s_0]} = [\alpha\beta^{-3}(s_0 +$

$\beta^3), \alpha)_{3, F[r_0, s_0]}$. In particular, this implies that C_Φ is Azumaya of rank 9. Consequently, the simple homomorphic images of C_Φ are determined by the maps taking $F[r, s]$ to $F[r_0, s_0]$ for \bar{F} -rational points (r_0, s_0) on the curve E_Δ , whose formula is given as above, and this provides a one-to-one correspondence between the Galois orbits of the \bar{F} -rational points on E_Δ and the simple homomorphic images of C_Φ . \square

In case $\beta = 0$, $\gamma \neq 0$ and furthermore $\delta \neq 0$, we can simply switch the roles of x and y and get a similar result to Theorem 5.14. What remains is the case of $\beta = \gamma = 0$.

THEOREM 5.15. *If $\beta = \gamma = 0$ then*

- (1) *The center of C_Φ is the polynomial ring $F[y_1]$.*
- (2) *The algebra $C_\Phi[y_1^{-1}]$ is Azumaya of rank 9 with the Laurent polynomial ring $F[y_1, y_1^{-1}]$ as its center.*
- (3) *There is a one-to-one correspondence between the Galois orbits of \bar{F}^\times and the simple homomorphic images of $C_\Phi[y_1^{-1}]$, taking each Galois orbit containing $s_0 \in \bar{F}^\times$ to $[\alpha(s_0^3 + \delta)s_0^{-3}, \alpha]_{3, F[s_0]}$.*
- (4) *The algebra C_Φ is not Azumaya.*

PROOF. In this case, the algebra C_Φ is an F -algebra generated by x, y_1, y_2 subject to the relations $x^3 = \alpha$, $[x, y_1] = [y_2, y_1] = 0$, $xy_2 - y_2x = y_1$ and $y_2^3 - y_1^3 = \delta$. Therefore y_1 is central in C_Φ and it generates over F a free algebra in one indeterminate.

The algebra $C_\Phi \otimes_{F[y_1]} q(F[y_1])$ contains the elements $z = xy_2y_1^{-1}$ and x . By a straight-forward calculation we see that $xz - zx = x$ and $z^3 - z = \alpha y_2^3 y_1^{-3}$. Since $y_2^3 - y_1^3 = \delta$, we obtain $z^3 - z = \alpha(\delta + y_1^3)y_1^{-3} \in q(F[y_1])$. Thus the $q(F[y_1])$ -subalgebra of $C_\Phi \otimes q(F[y_1])$ generated by x, z is cyclic of degree 3, and since it contains all the generators of C_Φ , we see that $q(F[y_1])[x, z] = C_\Phi \otimes q(F[y_1])$. Therefore the center of $C_\Phi \otimes q(F[y_1])$ is $q(F[y_1])$, and hence the center of C_Φ is $F[y_1]$.

Let A be a simple homomorphic image of $C_\Phi[y_1^{-1}]$. The image of y_1 in A is some element $s_0 \in \bar{F}^\times$. Let x' and y_2' be the images of x and y_2 in A . Now, x' and $z' = x'y_2's_0^{-1}$ generate a cyclic $F[s_0]$ -subalgebra of degree 3, and since they also generate A over $F[s_0]$, we conclude that A is a cyclic algebra over $F[s_0]$ of degree 3 with the symbol presentation $[z'^3 - z', x'^3]_{3, F[s_0]} = [\alpha(s_0^3 + \delta)s_0^{-3}, \alpha]_{3, F[s_0]}$. Therefore $C_\Phi[y_1^{-1}]$ is Azumaya of rank 9 and the statement (3) follows.

The algebra C_Φ is not Azumaya, however, because there is one image that is obtained by sending y_1 to 0, namely the commutative F -algebra generated by the images \bar{x}, \bar{y}_2 of x, y_2 , satisfying $\bar{x}^3 = \alpha, \bar{y}_2^3 = \delta$. \square

5.2.2. $e \neq 0$. By changing the variable X with $X' = eX$, we could assume that $e = 1$ in the first place. Now, by choosing the new pair of variables $X' = X + Y$ and $Y' = X - Y$, we then may assume the polynomial Φ is of the form

$$\Phi(Z, X, Y) = Z^3 - (X^2 - Y^2)Z - (\alpha X^3 + \beta X^2 Y + \gamma X Y^2 + \delta Y^3).$$

The algebra C_Φ thus in this case is

$$F\langle x, y : x^3 - x = \alpha, y^3 + y = \delta, x^2 * y - y = \beta, x * y^2 + x = \gamma \rangle.$$

The element x is Artin-Schreier. According to Lemma 2.19, $y = y_0 + y_1 + y_2$ such that $y_k x - x y_k = k y_k$ for $k = 0, 1, 2$. Substituting that in $x^2 * y - y = \beta$ leaves $y_0 = -\beta$. From $x * y^2 + x = \gamma$ we then obtain $y_1 y_2 - y_2 y_1 + x = \gamma$. Furthermore, a straight-forward calculation shows that $y^3 + y = \delta$ becomes

$$(27) \quad y_1^3 + y_2^3 = \delta + \beta^3 + \beta.$$

One can check that $w = y_2 y_1 - x^2 + (1 - \gamma)x$, y_1^3 and y_2^3 are central in C_Φ .

LEMMA 5.16. *The subalgebra $F[w, y_1^3]$ of the center of C_Φ is isomorphic to the coordinate ring of the affine curve*

$$E : s^2 = r^3 + r^2 - (\gamma^2 + \gamma)r - \alpha^2 - \alpha\gamma^3 + \alpha\gamma + (\delta + \beta^3 + \beta)^2.$$

In particular it is an integral domain.

PROOF. A straight-forward calculation shows that

$$\begin{aligned} w^3 &= y_2^3 y_1^3 + w^2 + (\gamma^2 + \gamma)w - \alpha^2 - \alpha\gamma^3 + \alpha\gamma \\ &= (\delta + \beta^3 + \beta)y_1^3 - y_1^6 + w^2 + (\gamma^2 + \gamma)w - \alpha^2 - \alpha\gamma^3 + \alpha\gamma. \end{aligned}$$

Thus $F[w, y_1^3]$ is the algebra over F generated by w and y_1^3 subject only to the relation in the equation above. The map defined by sending r, s to $-w, y_1^3 + (\delta + \beta^3 + \beta)$ then gives an F -algebra isomorphism. \square

THEOREM 5.17. *Assuming that $\delta + \beta^3 + \beta \neq 0$,*

- (1) *The algebra C_Φ is Azumaya of rank 9.*
- (2) *The center of C_Φ is the subalgebra $F[w, y_1^3]$, which is isomorphic to the coordinate ring of E .*
- (3) *There is a one-to-one correspondence between the Galois orbits of \bar{F} -rational points on E and the simple homomorphic images of C_Φ , taking each Galois orbit containing point (r_0, s_0) to the algebra $[\alpha, s_0 - (\delta + \beta^3 + \beta)]_{3, F[r_0, s_0]}$ if $s_0 \neq \delta + \beta^3 + \beta$, and to $[-\alpha, \delta + \beta^3 + \beta]_{3, F[r_0]}$ if $s_0 = \delta + \beta^3 + \beta$.*

PROOF. The element y_1 is invertible in $C_\Phi \otimes_{F[w, y_1^3]} q(F[w, y_1^3])$, and so inside this algebra $y_2 = (w + x^2 - (1 - \gamma)x)y_1^{-1}$. Thus $C_\Phi \otimes q(F[w, y_1^3])$ is generated over $q(F[w, y_1^3])$ by x and y_1 . Since x is Artin-Schreier, y_1^3 is central and $y_1x - xy_1 = y_1$, the algebra $C_\Phi \otimes q(F[w, y_1^3])$ is the cyclic algebra $[\alpha, y_1^3]_{3, q(F[w, y_1^3])}$. Thus the center of C_Φ being the intersection of C_Φ and the center of $C_\Phi \otimes q(F[w, y_1^3])$ is $F[w, y_1^3]$.

Every homomorphism from C_Φ to a simple algebra A takes $F[w, y_1^3]$ to a field $F[r_0, s_0]$ where (r_0, s_0) is an \bar{F} -rational point on the affine curve E and y_1^3 is sent to $s_0 - (\delta + \beta^3 + \beta)$ by the lemma above. If $s_0 \neq \delta + \beta^3 + \beta$ then A is generated by the images x', y'_1 of x, y_1 such that A is the cyclic algebra $[x'^3 - x', y_1'^3]_{3, F[r_0, s_0]} = [\alpha, s_0 - (\delta + \beta^3 + \beta)]_{3, F[r_0, s_0]}$. If $s_0 = \delta + \beta^3 + \beta$ then y_1^3 is sent to 0 and hence y_2 is sent to the invertible element $s_0 = \delta + \beta^3 + \beta$ by Equation (27). This means that A is generated by the images x', y'_2 of $-x, y_2$, satisfying $y'_2x' - x'y'_2 = y'_2$. Thus A is the cyclic algebra $[x'^3 - x', y_2'^3]_{3, F[r_0]} = [-\alpha, \delta + \beta^3 + \beta]_{3, F[r_0]}$. In particular, it implies that C_Φ is Azumaya of rank 9 and the statement (3) follows. \square

REMARK 5.18. If $\delta + \beta^3 + \beta = 0$ then for similar arguments as in the last proof, $C_\Phi[y_1^{-3}]$ is Azumaya of rank 9, and there is a one-to-one correspondence between its simple homomorphic images and the Galois orbits of the \bar{F} -rational points (r_0, s_0) on E with $s_0 \neq 0$, taking each such Galois orbit to the algebra $[\alpha, s_0]_{3, F[r_0, s_0]}$.

In this case, the algebra C_Φ is not necessarily Azumaya, for instance if furthermore $\gamma^3 - \gamma - \alpha = 0$ then F is a simple homomorphic image of C_Φ , and then C_Φ is definitely not Azumaya.

6. The Clifford Algebra of a Degree d Projective Variety

Let d be an integer, F a field and A a central simple F -algebra.

In this section we present a further generalization of the Clifford algebra of a monic polynomial, namely the Clifford algebra of a degree d projective variety.

Assume that V is a projective subvariety of A , i.e there exists a set of equations S , such that $V = \{u_1v_1 + \cdots + u_nv_n : (u_1, \dots, u_n) \in Z(S)\}$ for some linearly independent $v_1, \dots, v_n \in A$. We call V a degree d variety if there exist forms f_1, \dots, f_d such that for each $1 \leq i \leq p$, f_i is a form of degree i with n variables, and

$$(a_1v_1 + \cdots + a_nv_n)^d = \sum_{k=1}^d f_k(a_1, \dots, a_n)(a_1v_1 + \cdots + a_nv_n)^{d-k}$$

for all $(a_1, \dots, a_n) \in Z(S)$.

The variety V is called p -central if $f_1 = \dots = f_{p-1} = 0$.

We define the Clifford algebra of V to be

$$C(V) = F[x_1, \dots, x_n : (a_1x_1 + \dots + a_nx_n)^d = \sum_{k=1}^d f_k(a_1, \dots, a_n)(a_1v_1 + \dots + a_nv_n)^{d-k} \forall (a_1, \dots, a_n) \in Z(S)]$$

As before, there is a natural epimorphism $C(V) \rightarrow F[V]$ taking x_i to v_i for each i .

Since the algebra only depends on the choice of S and f_1, \dots, f_d , one can address the algebra as C_{S, f_1, \dots, f_p} .

If $f_1 = \dots = f_{d-1} = 0$ then the original variety V is d -central in A . In this case we may write $C_{S, f}$ to denote the Clifford algebra.

If $S = \emptyset$ then $C_{S, f}$ is simply the standard Clifford algebra C_f .

In this section we shall focus on the case of $d = 2$ and $f_1 = 0$.

REMARK 6.1. *It is easy to show that if $\text{char}(F) \neq 2$ and V is a degree 2 variety then $\{v - \frac{\text{Tr}(v)}{2} : v \in V\}$ is a 2-central variety. Therefore, in case of $d = 2$, we can assume that $f_1 = 0$ from the beginning.*

Let us have a look for example at $V = \{u_1v_1 + u_2v_2 + u_3v_3 : (u_1, u_2, u_3) \in Z(S)\}$ with $S = \{u_1u_3 - u_2^2\}$ and $(u_1v_1 + u_2v_2 + u_3v_3)^2 = f(u_1, u_2, u_3)$ for some ternary quadratic form f .

Because of the relation $u_1u_3 - u_2^2 \in S$,

$$(u_1x_1 + u_2x_2 + u_3x_3)^2 = u_1^2x_1^2 + u_2^2(x_2^2 + x_1 * x_3) + u_3^2x_3^2 + u_1u_2x_1 * x_2 + u_2u_3x_2 * x_3.$$

Consequently, $C_{S, f}$ is the algebra generated over F by x_1, x_2, x_3 subject to the following relations:

- (1) $x_1^2 = \alpha_{1,1}$
- (2) $x_3^2 = \alpha_{3,3}$
- (3) $x_1 * x_3 + x_2^2 = \alpha_{2,2} + \alpha_{1,3}$
- (4) $x_1 * x_2 = \alpha_{1,2}$
- (5) $x_2 * x_3 = \alpha_{2,3}$

where for each $1 \leq j, k \leq 3$, $\alpha_{j,k}$ is the coefficient of u_ju_k in f .

Therefore, $C_{S, f}$ is exactly the algebra associated to the quartic form $g(x) = \alpha_{3,3}x^4 + \alpha_{2,3}x^3 + (\alpha_{2,2} + \alpha_{1,3})x^2 + \alpha_{1,2}x + \alpha_{1,1}$, as defined in [HH07].

In that paper, Haile and Han proved that all the simple images of $C_{S,f}$ are quaternion algebras. We will now generalize this result to any 2-central variety with simultaneously diagonalizable defining equations.

THEOREM 6.2. *Let V be a 2-central variety with defining equations S and exponentiation form f . If S are simultaneously diagonalizable then the images of $C_{S,f}$ are all tensor products of up to $\lfloor \frac{n}{2} \rfloor$ quaternion algebras.*

PROOF. We can assume that S is a system of diagonal equations, because diagonalizing the system corresponds to a linear change of the generators of the Clifford algebra, and it does not change the algebra. For any $k \neq m$, x_m and x_k satisfy a relation $x_m x_k + x_k x_m = \alpha_{k,m}$. Consequently, $x_k^2 x_m = x_k(-x_m x_k + \alpha_{k,m}) = \alpha_{k,m} x_k - x_k x_m x_k = \alpha_{k,m} - (-x_m x_k + \alpha_{k,m}) x_k = x_m x_k^2$. Therefore, x_k^2 commutes with every x_m . Hence x_k^2 is in the center of $C_{S,f}$. Consequently, in every simple image of the algebra, $Fx_1 + \cdots + Fx_n$ is a 2-central space, and so the image is a tensor product of up to $\lfloor \frac{n}{2} \rfloor$ quaternion algebras. \square

COROLLARY 6.3. *In case of $\text{char}(F) \neq 2$, if S contains one equation then it is diagonalizable and therefore all the images of $C_{S,f}$ are tensor products of quaternion algebras. In particular, the algebra studied by Haile and Han in [HH07] satisfies this property.*

CHAPTER 2

d -Central Spaces in Tensor Products of Cyclic Algebras

1. Background

Let d be an integer, and F be an infinite field of characteristic prime to d containing a primitive d th root of unity ρ .

Let A be a tensor product of n cyclic algebras of degree d , $(\alpha_1, \beta_1)_{d,F} \otimes \cdots \otimes (\alpha_n, \beta_n)_{d,F} = F[x_1, y_1] \otimes \cdots \otimes F[x_n, y_n]$.

Let $V_0 = F$ and $V_k = F[x_k]y_k + V_{k-1}x_k$ for any $1 < k \leq n$. Assume that $v^d \in F$ for all $v \in V_{k-1}$ for a certain k . Every element of V_k is of the form $f(x_k)y_k + vx_k$ for some $f(x_1) \in F[x_1]$ and $v \in V_{k-1}$. Since v commutes with x_k and y_k , and $y_kx_k = \rho x_ky_k$, $(f(x_k)y_k + vx_k)^d = (f(x_k)y_k)^d + v^d x_k^{da_k} = N_{F[x_k]/F}(f(x_k))y_k^d + v^d x_k^{da_k} \in F$ (see [CV12, Remark 2.5]). For any $1 \leq m \leq d-1$, if $f(x_k) \neq 0$ then the eigenvector of $(f(x_k)y_k + vx_k)^m$ corresponding to the eigenvalue ρ^m with respect to conjugation by x_k is $(f(x_k)y_k)^m$, which is not zero, and therefore $(f(x_k)y_k + vx_k)^m \notin F$. If $f(x_k) = 0$ then what is left is vx_k , and of course $v^m x_k^m \notin F$. Consequently, V_k is d -central. Since $V_0 = F$, by induction V_k is d -central for every $1 \leq k \leq n$. The dimension of each V_k is $dk + 1$.

For $d = 2$, it follows from the theory of Clifford algebras that for any $k \leq n$, V_k is maximal with respect to inclusion. Furthermore, it is known that every maximal space is of some odd dimension $2k + 1$ and can be obtained in the same way as V_k by some decomposition of the algebra as a tensor product of quaternion algebras.

In [MV12], Matzri and Vishne noted that for $d = 3$ and $n = 1$, every maximal 3-central space is a subspace of V_1 .

In Section 2 we prove that each V_K is maximal with respect to inclusion when $d = p$ for some prime p . In Section 3 we focus on one cyclic algebra of degree p^k where p is prime and show that it contains a family of p^k -subspaces, of which V_1 is a special case.

A finite set $B = \{b_1, \dots, b_n\} \subseteq A$ consisting of F -linearly independent invertible elements is called a **p -central set** if

- (1) For any $1 \leq k \leq n$, $b_k^p = \alpha_k \in F$.
- (2) For any $1 \leq m < k \leq n$, $b_m b_k = \rho^{c_{m,k}} b_k b_m$ for some $c_{m,k} \in \mathbb{Z}$.

This term was introduced by Rowen in [Row88, Vol II, pp. 248-251]. A p -central pair is a p -central set of cardinality 2.

It is known that every nondegenerate quadratic space is spanned by a 2-central set. Therefore it generates a tensor product of quaternion algebras.

In [Rac09], Raczek proved that every 3-dimensional 3-central subspace of a cyclic algebra of degree 3 is of the form $F\mu + F\nu + F(\lambda_1\mu\nu^2 + \lambda_2\mu^2\nu^2)$ where μ and ν form a 2-central pair.

In Section 4 we prove that 5 is the maximal dimension of a 4-central subspace of a cyclic algebra of degree 4 containing a 4-central pair. In Section 5 we classify p -central subspaces of cyclic algebras of degree p containing p -central sets of the form $\{x, y, xy\}$ and 5-central spaces containing any 5-central set of size 3.

Section 6 is dedicated to 3-central spaces spanned by 3-central sets.

In Section 7 we study the effect of the existence of 3-central spaces in algebras of fixed degrees. We focus on degree 3. We show that for a field extension K/F , if a central simple K -algebra A of degree 3 contains an F -vector subspace V such that $v^3 \in F$ for all $v \in V$ and $[V : F] = 3$ then A is a restriction of a central simple F -algebra. We provide a counterexample in case $[V : F] = 2$.

2. Maximal p -Central Spaces

Here we shall assume that $d = p$ for some prime p . The following result appeared in my Master's thesis [Cha09] and is repeated here in a refined manner for completeness.

THEOREM 2.1. *For any $k \leq n$, V_k is maximal with respect to inclusion.*

PROOF. Let $V = V_k$. V has a standard basis

$$B = \{x_i^j y_i x_{i+1} \dots x_k : 1 \leq i \leq k, 0 \leq j \leq p-1\} \cup \{x_1 x_2 \dots x_k\}.$$

Let z be a nonzero element in the algebra A . This element can be expressed as a linear combination of the monomials $x_1^{c_1} y_1^{e_1} \dots x_n^{c_n} y_n^{e_n}$. Let us assume negatively that $V + Fz$ is p -central. Consequently, $w^{p-1} * z \in F$ for every $w \in B$. Since we can subtract from z the appropriate linear combination of the elements of B , we can assume that $w^{p-1} * z = 0$ for every $w \in B$.

Let us pick one monomial $t = x_1^{c_1} y_1^{e_1} \dots x_n^{c_n} y_n^{e_n}$.

If $e_1 = e_2 = \dots = e_n = 0$ then t commutes with $x_1 x_2 \dots x_k \in V$. Since $(x_1 x_2 \dots x_k)^{p-1} * z = 0$, the coefficient of t in z is zero.

Otherwise, let i be the maximal integer for which $e_i \neq 0$. The monomial t commutes with the element $x_i^r y_i x_{i+1} \dots x_k \in V$ where $r \equiv c_i e_i^{-1} \pmod{p}$. Since $(x_i^r y_i x_{i+1} \dots x_k)^{p-1} * z = 0$, the coefficient of t in z is zero.

Therefore, the coefficient of t in z is always zero, which means that $z = 0$, and that is a contradiction. \square

3. Family of p^k -Central Spaces

Assume $d = p^k$ for some prime p . In a cyclic algebra $A = F[x, y] = (\alpha, \beta)_{d, F}$ there is a d -central space of the form V_1 as defined above. Apparently this space belongs to a larger family of d -central subspaces of this algebra.

Let $V = F[x^{p^e}]y + F[y^{p^{k-e}}]x$ for some $0 \leq e \leq k-1$.

PROPOSITION 3.1. *The space V is p^k -central.*

PROOF. Every element in V is of the form $f(x^{p^e})y + g(y^{p^{k-e}})x$ where f and g are polynomials. Its p^k th power is $(N_{F[x^{p^e}]/F}(f(x^{p^e})))^{p^{k-e}}\beta + (N_{F[y^{p^{k-e}}]/F}(g(y^{p^{k-e}})))^{p^e}\alpha \in F$. It is clear that the lower powers are not in the center. \square

CONJECTURE 3.2. *The p^k -central space V is maximal with respect to inclusion.*

Idea: Assume to the contrary, that there exists $z \in A \setminus V$ such that $V + Fz$ is p^k -central. Let $0 \leq i, n \leq p^e - 1$, $0 \leq j, m \leq p^{k-e} - 1$. We consider the coefficient of the monomial $x^{i+jp^e} y^{m+np^{k-e}}$ in z . If $i = j = 0$ then the monomial commutes with y and therefore its coefficient in z is zero. Similarly if $m = n = 0$ then the coefficient is zero.

If $i = m = 0$ and $n, j \neq 0$ then the relation

$$\text{Tr}(z * (x^{(p^{k-e}-j)p^e} y) * y^{p^k - np^{k-e} - 1}) = 0$$

holds, because $1 \leq 1 + 1 + p^k - np^{k-e} - 1 \leq p^k - 1$.

If $i = 0$, $m = 1$ and $n = 0$ then $x^{i+jp^e} y^{m+np^{k-e}} \in V$ which means that we can assume its coefficient in z is zero.

If $i = 0$ and $m \geq 2$ then the relation

$$\text{Tr}(z * (x^{(p^{k-e}-j)p^e} y) * y^{p^k - m - 1 - np^{k-e}}) = 0$$

holds, because $1 \leq 1 + 1 + p^k - m - 1 - np^{k-e} \leq p^k - 1$.

Similar relations hold if $m = 0$, $i = 1$ and $j = 0$ or $m = 0$ and $i \geq 2$. This covers all the options with either $i = 0$ or $m = 0$,

Let us assume that $i, m \neq 0$. Therefore the relation

$$\text{Tr}(z * (x^{(p^{k-e}-j-1)p^e} y) * y^{p^{k-e}-m-1} * (y^{(p^e-n-1)p^{k-e}} x) * x^{p^e-i-1}) = 0$$

holds, because $1 + 1 + p^{k-e} - m - 1 + 1 + p^e - i - 1 \leq p^e + p^{k-e} - 1 \leq p^k - 1$.

If we manage to prove that all the relations above are nontrivial then it will mean that $z = 0$.

REMARK 3.3. *In case of $p = k = 2$ all the relations above turn out to be nontrivial, and the 4-central spaces are indeed maximal.*

4. 5-Dimensional 4-Central Spaces

Let A be a central division algebra of degree 4 over a field F containing a primitive fourth root of unity i and of characteristic not 2.

The aim of this section is to prove the following theorem:

THEOREM 4.1. *The upper bound for the dimension of 4-central spaces containing pairs of standard generators is 5.*

The rest of this section will deal with proving this theorem. Assume to the contrary, that there exists a 6-dimensional 4-central space W containing a pair x and y satisfying $yx = ixy$. For any element $q \in W$ we write $q = \sum_{m=0}^3 \sum_{n=0}^3 q_{m,n} x^m y^n$. From $\text{Tr}(q) = 0$ we get $q_{0,0} = 0$. Because $\text{Tr}(x * y * q) = 0$ we always get $q_{3,3} = 0$. There exists a subspace V of dimension 5 such that for every $q \in V$, $q_{2,2} = 0$. Since $\text{Tr}(x^k * q) = \text{Tr}(y^k * q) = 0$ for $k = 1, 2$, and we can always subtract $q_{1,0}x + q_{0,1}y$ from q , we have $V = Fx + Fy + V'$ such that $V' = \{q \in V : q_{k,0} = q_{0,k} = 0 \forall k\}$.

PROPOSITION 4.2. *The projection of V on $Fxy + Fxy^2 + Fx^2y$ is of dimension no greater than 2.*

PROOF. Assume to the contrary, that it is of dimension 3. Then there exist $z, w, t \in V$ such that $z_{1,1}, w_{1,2}, t_{2,1} \neq 0$ while $z_{1,2} = z_{2,1} = w_{1,1} = w_{2,1} = t_{1,1} = t_{1,2} = 0$. From $\text{Tr}(w^2 * y) = 0$ we get $w_{3,1} = 0$. From $\text{Tr}(w^2) = 0$ we get $w_{3,2} = 0$. From $\text{Tr}(w^3) = 0$ we get $w_{1,3} = 0$ or $w_{2,3} = 0$. Similarly, $t_{1,3} = t_{2,3} = 0$ and either $t_{3,1} = 0$ or $t_{3,2} = 0$. From $\text{Tr}(w * t * x) = 0$ we get $w_{1,3} = 0$ and from $\text{Tr}(w * t * y) = 0$ we get $t_{3,1} = 0$. From $\text{Tr}(z * t * x) = 0$ we get $z_{1,3} = 0$. From $\text{Tr}(z * w * y) = 0$ we get $z_{3,1} = 0$. From $\text{Tr}(z * w) = 0$ we get $z_{3,2} = 0$ and from $\text{Tr}(z * t) = 0$ we

get $z_{2,3} = 0$. Consequently, $z = z_{1,1}xy$. But then from $\text{Tr}(z * w * t) = 0$ we get $z_{1,1}w_{1,2}t_{2,1} = 0$, a contradiction. \square

COROLLARY 4.3. *V' contains an element z of the form $z = z_{1,3}xy^3 + z_{2,3}x^2y^3 + z_{3,2}x^3y^2$ or $z = z_{3,1}x^3y + z_{2,3}x^2y^3 + z_{3,2}x^3y^2$.*

PROOF. The projection of V' on $Fxy + Fxy^2 + Fx^2y$ is of dimension no greater than 2. Therefore there exists a nonzero element $z \in V'$ in the kernel of this projection, i.e. $z_{1,1} = z_{1,2} = z_{2,1} = 0$. Since $\text{Tr}(z^k) = \text{Tr}((z_{1,3}xy^3 + z_{3,1}x^3y)^k)$ for $k = 2, 3$, $z_{1,3}xy^3 + z_{3,1}x^3y$ must also be 4-central. Therefore, since $z_{1,3}xy^3 + z_{3,1}x^3y$ is in the cyclic field extension $F[x^3y]/F$ of degree 4, $z_{3,1} = 0$ or $z_{1,3} = 0$. \square

THEOREM 4.4. *V is of the form $F[\mu]\nu + F\mu$ where $\mu\nu = i^k\nu\mu$ for $k = \pm 1$.*

PROOF. Without loss of generality, V' contains some nonzero z of the form $z = z_{3,1}x^3y + z_{2,3}x^2y^3 + z_{3,2}x^3y^2$.

Let us assume that $z_{3,1}, z_{2,3} \neq 0$.

Let q be an arbitrary element in V' . We can assume that $q_{3,1} = 0$.

From $\text{Tr}(z * q * x) = 0$ we get $q_{1,1} = 0$. From $\text{Tr}(z * q * y) = 0$ we get $q_{1,2} = 0$.

Let us assume negatively that $q_{2,1} \neq 0$. From $\text{Tr}(q^2 * x) = 0$ we get $q_{1,3} = 0$. From $\text{Tr}(q^2) = 0$ we get $q_{2,3} = 0$. But then $\text{Tr}(q * z) = 0$ yields $q_{2,1}z_{2,3} = 0$, a contradiction. Consequently, $q_{2,1} = 0$. Like in Corollary 4.3, q is of the form $q = q_{1,3}xy^3 + q_{2,3}x^2y^3 + q_{3,2}x^3y^2$ or $q = q_{3,1}x^3y + q_{2,3}x^2y^3 + q_{3,2}x^3y^2$. Since the same holds also for $q + z$, q must be of the form $q = q_{3,1}x^3y + q_{2,3}x^2y^3 + q_{3,2}x^3y^2$. Hence, $V' = Fx^3y + Fx^2y^3 + Fx^3y^2$.

Let us assume that $z_{3,1} = 0$ and $z_{3,2}, z_{2,3} \neq 0$. We have $V' = V'' + Fz$. Let us assume negatively that the projection of V'' on $Fx^2y + Fxy^2$ is of dimension two. Let q be an arbitrary element of V'' . From $\text{Tr}(z * q) = 0$ we get $q_{2,1}z_{2,3} + q_{1,2}z_{3,2} = 0$. But that is a contradiction. Therefore the projection of V'' on $Fx^2y + Fxy^2$ is of dimension no greater than 1. Consequently, V'' contains an element q where $q_{1,2} = q_{2,1} = 0$. From $\text{Tr}(q * z * x) = 0$ we get $q_{1,1} = 0$. Then by similar arguments to Corollary 4.3 and the previous paragraph, q must be of the form $q = q_{3,1}x^3y + q_{2,3}x^2y^3 + q_{3,2}x^3y^2$. Hence, $V' = Fx^3y + Fx^2y^3 + Fx^3y^2$. If $q_{3,1} \neq 0$ or $q_{1,3} \neq 0$ then we are done. Otherwise, $Fq + Fz = Fx^3y^2 + Fx^2y^3$. We shall later solve this case separately.

Let us assume that $z_{3,1}, z_{3,2} \neq 0$ and $z_{2,3} = 0$. We have $V' = V'' + Fz$. Let q be an arbitrary element of V'' . From $\text{Tr}(z * q * y) = 0$ we get

$iq_{1,1}z_{3,2} + q_{1,2}z_{3,1} = 0$. From $\text{Tr}(z * q) = 0$ we get $iq_{1,2}z_{3,2} + q_{1,3}z_{3,1} = 0$. Since V'' is of dimension 2, and its projection on $Fxy + Fxy^2 + Fxy^3$ is of dimension at most one, we can assume that $q_{1,1} = q_{1,2} = q_{1,3} = 0$. We can also assume that $q_{3,1} = 0$. We claim that $q_{2,1} = 0$. Assume to the contrary. From $\text{Tr}(q^2) = 0$ we get $q_{2,3} = 0$. Therefore $q = q_{2,1}x^2y + q_{3,2}x^3y^2$. From $\text{Tr}(q * z^2) = 0$ we get $q_{2,1}z_{3,1}z_{3,2} = 0$, a contradiction. Therefore $q_{2,1} = 0$. Then for similar reasons as in Corollary 4.3 q must be of the form $q = q_{3,1}x^3y + q_{2,3}x^2y^3 + q_{3,2}x^3y^2$. If $q_{3,1} \neq 0$ or $q_{1,3} \neq 0$ then we are done. Otherwise, $Fq + Fz = Fx^3y^2 + Fx^2y^3$. We shall later solve this case separately.

What remains is to check the cases of $z = z_{3,1}x^3y$ and $z = z_{3,2}x^3y^2$ separately. (The case of $z = z_{2,3}x^2y^3$ is similar to the latter.)

Let us assume that $z = z_{3,2}x^3y^2$. We have $V' = V'' + Fz$ where $V'' = \{v \in V : \text{Tr}(z^4v) = 0\}$. Let q be an arbitrary element of V'' . In particular, $q_{3,2} = 0$. From $\text{Tr}(q * z * y) = 0$ we get $q_{1,1} = 0$. From $\text{Tr}(q * z) = 0$ we get $q_{1,2} = 0$. We claim that $q_{2,1} = 0$. Assume to the contrary. From $\text{Tr}(q^2 * x) = 0$ we get $q_{1,3} = 0$. From $\text{Tr}(q^2) = 0$ we get $q_{2,3} = 0$. Then $q = q_{2,1}x^2y + q_{3,1}x^3y$. Since the dimension of V'' is two, we can assume that $q_{3,1} \neq 0$. But then from $\text{Tr}(q^2 * z) = 0$ we get $q_{2,1}q_{3,1}z = 0$, a contradiction. Therefore $q_{2,1} = 0$. Then for similar reasons as in Corollary 4.3, q must be of the form $q = q_{3,1}x^3y + q_{2,3}x^2y^3$ or $q = q_{1,3}xy^3 + q_{2,3}x^2y^3$. V'' is spanned by q and some element t . If $q = q_{3,1}x^3y + q_{2,3}x^2y^3$ then t must also be of the form $t = t_{3,1}x^3y + t_{2,3}x^2y^3$, and if $q = q_{1,3}xy^3 + q_{2,3}x^2y^3$ then t must also be of the form $t = t_{1,3}xy^3 + t_{2,3}x^2y^3$. Hence, $V'' = Fx^3y + Fx^2y^3$ or $V'' = Fxy^3 + Fx^2y^3$. Consequently, $V = F[x^3y]y + Fx^3y$ or $V = F[xy^3]y + Fxy^3$.

Let us assume that $z = z_{3,1}x^3y$. We have $V' = V'' + Fz$. Let q be an arbitrary element of V'' . We can assume that $q_{3,1} = 0$. From $\text{Tr}(z * q) = 0$ we get $q_{1,3} = 0$. From $\text{Tr}(z * q * y) = 0$ we get $q_{1,2} = 0$. Assume $q_{2,1} \neq 0$. Then from $\text{Tr}(q^2) = 0$ we get $q_{2,3} = 0$. Assuming $q_{3,2} \neq 0$ would lead to a contradiction because then $\text{Tr}(q^2 * z) = 0$ implies $z_{3,1}q_{3,2}q_{2,1} = 0$. Consequently, $q_{3,2} = 0$. Now, V'' is spanned by q and some element t . We can assume that $t_{2,1} \neq 0$ too. Then $t = t_{1,1}xy + t_{2,1}x^2y$, and $V'' = Fxy + Fx^2y$. In this case $V = F[x]y + Fx$. Assume $q_{2,1} = 0$. Then for similar reasons as in Corollary 4.3 q must be of the form $q = q_{2,3}x^2y^3 + q_{3,2}x^3y^2$. Hence $V'' = Fx^2y^3 + Fx^3y^2$ and $V = F[x^3y]y + Fx^3y$. \square

The space V as described in the last theorem is maximal, and therefore not contained in a larger 4-central space W , contradiction.

5. p -Central Spaces containing p -Central Sets of Size 3

Let p be a prime number, F be an infinite field of characteristic not p containing a primitive p th root of unity, ρ . Let A be a cyclic algebra of degree p . Let V be some p -central F -vector subspace of A of dimension at least 4. Assume that V contains a p -set of cardinality 3. By replacing ρ with some ρ^k for some integer k , we can assume that V contains x, y and $x^i y^j$ for some integers i, j where $A = F[x, y : x^p = \alpha, y^p = \beta, yx = \rho xy]$. We would like to prove that $V \subseteq F[w]z + Fw$ for some $w, z \in A$ such that $wz = \rho^k zw$ for some integer k . So far, we have managed to do it assuming either $p = 5$ or that one element in the p -central set is a product of the two others (i.e. $i = j = 1$).

5.1. One element is the product of the two others. Assume $i = j = 1$.

THEOREM 5.1. *The space V is contained in either $F[x]y + Fx$ or $F[y]x + Fy$.*

PROOF. We have $V = Fx + Fy + Fxy + Fz$ for some z . For any $a, b, c, d \in F$ and any $0 < k < p$, $\text{Tr}((ax + by + cxy + dz)^k) = 0$. Consequently, $\text{Tr}(x^i * y^j * (xy)^m * z^n) = 0$ for any $0 < i + j + m + n < p$. There is the decomposition $z = \sum z_{i,j}$ such that $z_{i,j} \in Fx^i y^j$.

How do we prove that if $i, j > 1$ then $z_{i,j} = 0$?

Without loss of generality, assume $i > j$. Now, $\text{Tr}(y^{i-j} * (xy)^{p-i} * z) = 0$, because $i - j + p - i + 1 = p - j + 1 < p$. However, $\text{Tr}(y^{i-j} * (xy)^{p-i} * z) = y^{i-j} * (xy)^{p-i} * z_{i,j}$. If $z_{i,j} \neq 0$ then $y^{i-j} * (xy)^{p-i} * z_{i,j} \neq 0$, because every monomial in this sum becomes ρ^t for some integer t , and the number of monomials in this sum is prime to p . Therefore, $z_{i,j} = 0$.

So far we proved that $z = z_{1,1} + \cdots + z_{1,p-1} + z_{2,1} + \cdots + z_{p-1,1}$.

Let us assume that $z_{i,1} \neq 0$ for some $i > 1$.

If $i > j$ then take $\text{Tr}(y^{i-j} * (xy)^{p-i-1} * z^2) = 0$. (This is true because $i - j + p - i - 1 + 2 = p - j + 1 < p$.) However $\text{Tr}(y^{i-j} * (xy)^{p-i-1} * z^2) = y^{i-j} * (xy)^{p-i-1} * z_{i,1} * z_{1,j}$. For the same reason as before (the number of summands is prime to p), this expression is zero if and only if either $z_{i,1} = 0$ or $z_{1,j} = 0$, which means that $z_{1,j} = 0$.

If $i < j$ then take $\text{Tr}(y^{j-i} * (xy)^{p-j-1} * z^2) = 0$ and continue similarly to prove that $z_{1,j} = 0$.

In conclusion, if V contains an element in $F[x]y + Fx$ that does not appear in $F[y]x + Fy$ then $V \subseteq F[x]y + Fx$. Conversely, if V contains an element in $F[y]x + Fy$ that does not appear on $F[x]y + Fx$ then $V \subseteq F[y]x + Fy$. \square

5.2. The degree five case. Assume now that $p = 5$.

THEOREM 5.2. *The space V is contained in one of the following: $F[x]y + Fx$, $F[y]x + Fy$ or $F[x^3y^2]x + F(x^3y^2)^i$ for some $1 \leq i \leq 4$.*

PROOF. The element $x^i y^j$ is contained in V . Therefore $i + j \leq 6$, because otherwise it contradicts the fact that $\text{Tr}(x^{5-i} * y^{5-j} * (x^i y^j)) = 0$. Furthermore, $\text{Tr}(x * y * (x^i y^j)^2) = 0$, which means that the case $i = j = 2$ is impossible. Consequently, the possibilities for $x^i y^j$ are xy^j , $x^i y$, $x^3 y^3$, $x^2 y^3$, $x^3 y^2$, $x^2 y^4$ and $x^4 y^2$.

Let $z \in V \setminus (Fx + Fy + Fx^i y^j)$. Since $\text{Tr}(x^{5-i} * y^{5-j} * (x^i y^j)) = 0$ for $i + j \geq 7$, $z = z_{1,1} + z_{1,2} + z_{1,3} + z_{1,4} + z_{2,1} + z_{3,1} + z_{4,1} + z_{2,2} + z_{2,3} + z_{3,2} + z_{3,3} + z_{2,4} + z_{4,2}$ where $z_{m,n} \in Fx^m y^n$.

Now, $0 = \text{Tr}(x * y * z^2) = \text{Tr}(x * y * z_{2,2}^2) + \text{Tr}(x * y * z_{1,3} * z_{3,1}) + \text{Tr}(x * y * z_{1,1} * z_{3,3}) + \text{Tr}(x * y * z_{1,2} * z_{3,2}) + \text{Tr}(x * y * z_{2,1} * z_{2,3})$. This means that if either $z_{1,3} = 0$ or $z_{3,1} = 0$, $z_{2,3} = 0$ or $z_{2,1} = 0$, $z_{1,2} = 0$ or $z_{3,2} = 0$ and either $z_{3,3} = 0$ or $z_{1,1} = 0$ then $z_{2,2} = 0$.

The case of $i = j = 1$ has already been dealt with in the Theorem 5.1.

Assume $x^i y^j = x^2 y$. $0 = \text{Tr}((x^2 y)^2 * y * z) = \text{Tr}((x^2 y)^2 * y * z_{1,2})$, and therefore $z_{1,2} = 0$. $0 = \text{Tr}((x^2 y)^2 * z) = \text{Tr}((x^2 y)^2 * z_{1,3})$, and therefore $z_{1,3} = 0$. $0 = \text{Tr}((x^2 y) * x^2 * z) = \text{Tr}((x^2 y) * x^2 * z_{1,4})$, and therefore $z_{1,4} = 0$. $0 = \text{Tr}((x^2 y) * x * y * z) = \text{Tr}((x^2 y) * x * y * z_{2,3})$, and therefore $z_{2,3} = 0$. $0 = \text{Tr}((x^2 y) * y^2 * z) = \text{Tr}((x^2 y) * y^2 * z_{3,2})$, and therefore $z_{3,2} = 0$. $0 = \text{Tr}((x^2 y) * y * z) = \text{Tr}((x^2 y) * y * z_{3,3})$, and therefore $z_{3,3} = 0$. $0 = \text{Tr}((x^2 y) * x * z) = \text{Tr}((x^2 y) * x * z_{2,4})$, and therefore $z_{2,4} = 0$. $0 = \text{Tr}((x^2 y)^3 * z) = \text{Tr}((x^2 y)^3 * z_{4,2})$, and therefore $z_{4,2} = 0$.

Since $z_{3,3} = z_{3,2} = z_{2,3} = z_{1,3} = 0$, $z_{2,2} = 0$.

Consequently, $V \subseteq F[x]y + Fx$.

Assume $x^i y^j = x^3 y$. $0 = \text{Tr}((x^3 y)^3 * z) = \text{Tr}((x^3 y)^3 * z_{1,2})$, and therefore $z_{1,2} = 0$. $0 = \text{Tr}((x^3 y)x * y * z) = \text{Tr}((x^3 y)x * y * z_{1,3})$, and therefore $z_{1,3} = 0$. $0 = \text{Tr}((x^3 y) * x * z) = \text{Tr}((x^3 y) * x * z_{1,4})$, and therefore $z_{1,4} = 0$. $0 = \text{Tr}((x^3 y) * y * z) = \text{Tr}((x^3 y) * y * z_{2,3})$, and therefore $z_{2,3} = 0$. $0 = \text{Tr}((x^3 y)^2 * x * z) = \text{Tr}((x^3 y)^2 * x * z_{3,3})$, and therefore $z_{3,3} = 0$. $0 = \text{Tr}((x^3 y) * z) = \text{Tr}((x^3 y) * z_{2,4})$, and therefore $z_{2,4} = 0$. $0 = \text{Tr}((x^3 y)^2 * y * z) = \text{Tr}((x^3 y)^2 * y * z_{4,2})$, and therefore $z_{4,2} = 0$.

Since $z_{1,2} = z_{1,3} = z_{2,3} = z_{3,3} = 0$, $z_{2,2} = 0$.

Since $\text{Tr}(x * (x^3 y) * z^2) = 0$, we have $x * (x^3 y) * z_{3,2}^2 = 0$, which means that $z_{3,2} = 0$, and therefore $V \subseteq F[x]y + Fx$.

Consequently, $V \subseteq F[x]y + Fx$.

Assume $x^i y^j = x^4 y$. then V must be a subspace of $F[x]y + Fx + F[x^4 y]x + Fx^4 y$ because the traces of the followings are nonzero: $0 = \text{Tr}((x^4 y) * y^2 * z) = \text{Tr}((x^4 y) * y^2 * z_{1,2})$, and therefore $z_{1,2} = 0$. $0 = \text{Tr}((x^4 y) * y * z) = \text{Tr}((x^4 y) * y * z_{1,3})$, and therefore $z_{1,3} = 0$. $0 = \text{Tr}((x^4 y)^2 * y * z) = \text{Tr}((x^4 y)^2 * y * z_{2,2})$, and therefore $z_{2,2} = 0$. $0 = \text{Tr}((x^4 y) * z) = \text{Tr}((x^4 y) * z_{1,4})$, and therefore $z_{1,4} = 0$. $0 = \text{Tr}((x^4 y)^2 * z) = \text{Tr}((x^4 y)^2 * z_{2,3})$, and therefore $z_{2,3} = 0$. $0 = \text{Tr}((x^4 y)^3 * z) = \text{Tr}((x^4 y)^3 * z_{3,2})$, and therefore $z_{3,2} = 0$.

Since $\text{Tr}(z^2) = 0$ we have either $z_{3,1} = 0$ or $z_{2,4} = 0$. Since $\text{Tr}(z^2 * y) = 0$ we have either $z_{2,1} = 0$ or $z_{3,3} = 0$. Since $\text{Tr}(z^2 * y^2) = 0$ we have either $z_{1,1} = 0$ or $z_{4,2} = 0$.

If $z_{3,1} = z_{2,1} = z_{4,2} = 0$ then since $\text{Tr}(z^3) = 0$, either $z_{1,1} = 0$ or $z_{3,3} = 0$, and since $\text{Tr}(z^3 * y) = 0$, either $z_{1,1} = 0$ or $z_{2,4} = 0$.

If $z_{3,1} = z_{1,1} = z_{3,3} = 0$ then since $\text{Tr}(z^3) = 0$, either $z_{2,1} = 0$ or $z_{4,2} = 0$, and since $\text{Tr}(z^2 * x) = 0$, either $z_{2,1} = 0$ or $z_{2,4} = 0$.

If $z_{1,1} = z_{2,1} = z_{2,4} = 0$ then since $\text{Tr}(z^3 * y) = 0$, either $z_{3,1} = 0$ or $z_{4,2} = 0$, and since $\text{Tr}(z^3 * x) = 0$, either $z_{3,1} = 0$ or $z_{3,3} = 0$.

Similarly, if $z_{3,1} = z_{3,3} = z_{4,2} = 0$ then either $z_{2,4} = 0$ or $z_{2,1} = z_{1,1} = 0$, if $z_{2,1} = z_{2,4} = z_{4,2} = 0$ then either $z_{3,3} = 0$ or $z_{3,1} = z_{1,1} = 0$, and if $z_{1,1} = z_{2,4} = z_{3,3} = 0$ then either $z_{4,2} = 0$ or $z_{3,1} = z_{2,1} = 0$.

All in all, V is contained in either $F[x]y + Fx$ or $F[x^4 y]x + Fx^4 y$.

Similarly, if $x^i y^j = xy^i$ for $i = 2$ or $i = 3$ then $V \subseteq F[y]x + Fy$, and if V contains xy^4 then either $V \subseteq F[y]x + Fy$ or $V \subseteq F[xy^4]y + Fxy^4$.

Assume $x^i y^j = x^2 y^3$. $0 = \text{Tr}((x^2 y^3) * x * y * z) = \text{Tr}((x^2 y^3) * x * y * z_{2,1})$, and therefore $z_{2,1} = 0$. $0 = \text{Tr}((x^2 y^3) * y * z) = \text{Tr}((x^2 y^3) * y * z_{3,1})$, and therefore $z_{3,1} = 0$. $0 = \text{Tr}((x^2 y^3)^3 * z) = \text{Tr}((x^2 y^3)^3 * z_{4,1})$, and therefore $z_{4,1} = 0$. $0 = \text{Tr}((x^2 y^3) x^2 * z) = \text{Tr}((x^2 y^3) x^2 * z_{1,2})$, and therefore $z_{1,2} = 0$. $0 = \text{Tr}((x^2 y^3)^2 * y * z) = \text{Tr}((x^2 y^3)^2 * y * z_{1,3})$, and therefore $z_{1,3} = 0$. $0 = \text{Tr}((x^2 y^3)^2 * z) = \text{Tr}((x^2 y^3)^2 * z_{1,4})$, and therefore $z_{1,4} = 0$. $0 = \text{Tr}((x^2 y^3) * z) = \text{Tr}((x^2 y^3) * z_{3,2})$, and therefore $z_{3,2} = 0$. $0 = \text{Tr}((x^2 y^3) * x * z) = \text{Tr}((x^2 y^3) * x * z_{2,2})$, and therefore $z_{2,2} = 0$.

Since $\text{Tr}(x * (x^2 y^3) * z^2) = 0$, $x * (x^2 y^3) * z_{1,1}^2 = 0$, which means that $z_{1,1} = 0$. Consequently, $V \subseteq F[x^2 y^3]y + Fx^2 y^3$.

Consequently, $V \subseteq F[x^2 y^3]y + Fx^2 y^3 + Fxy$

Similarly, if $x^i y^j = x^3 y^2$ then $V \subseteq F[x^3 y^2]x + Fx^3 y^2$.

Assume $x^i y^j = x^2 y^4$. $0 = \text{Tr}((x^2 y^4)^2 * y * z) = \text{Tr}((x^2 y^4)^2 * y * z_{1,1})$, and therefore $z_{1,1} = 0$. $0 = \text{Tr}((x^2 y^4)^2 * x * z) = \text{Tr}((x^2 y^4)^2 * x * z_{2,1})$, and therefore $z_{2,1} = 0$. $0 = \text{Tr}((x^2 y^4)^2 * z) = \text{Tr}((x^2 y^4)^2 * z_{1,2})$, and

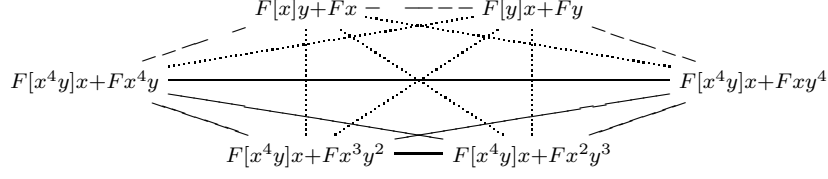


FIGURE 1. The maximal 5-central spaces containing $x, y, x^i x^j$ and the dimensions of their intersections. A continuous line stands for intersection of dimension 5, a broken line for 3 and a dotted line for 2.

therefore $z_{1,2} = 0$. $0 = \text{Tr}((x^2 y^4)^2 * x * z) = \text{Tr}((x^2 y^4)^2 * x * z_{1,3})$. $0 = \text{Tr}((x^2 y^4) * z) = \text{Tr}((x^2 y^4) * z_{3,1})$, and therefore $z_{3,1} = 0$.

Since $z_{1,1} = z_{2,1} = z_{1,2} = z_{1,3} = 0$, $z_{2,2} = 0$.

Since $\text{Tr}(x * (x^2 y^4) * z^2) = 0$, $x * (x^2 y^4) * z_{1,3}^2 = 0$, which means that $z_{1,3} = 0$.

Now, $\text{Tr}(z^k) = \text{Tr}((z_{3,2} + z_{2,3} + z_{4,1} + z_{1,4})^k)$ for $1 \leq k \leq 4$. Therefore, since z is 5-central, so is $z_{3,2} + z_{2,3} + z_{4,1} + z_{1,4}$. However, this is an element of the field $F[(xy^4)^k : k \neq 0]$. Consequently, all of the four summands but one are equal to zero. Hence $V \subseteq F[xy^4]x + F(xy^4)^k$ for some $1 \leq k \leq 4$.

Similarly, if $x^i y^j = x^4 y^2$ then $V \subseteq F[xy^4]x + F(xy^4)^k$ for some $1 \leq k \leq 4$.

Assume $x^i y^j = x^3 y^3$. $0 = \text{Tr}(x * y * (x^3 y^3) * z) = \text{Tr}(x * y * (x^3 y^3) * z_{1,1})$, and therefore $z_{1,1} = 0$. $0 = \text{Tr}(x * (x^3 y^3) * z) = \text{Tr}(x * (x^3 y^3) * z_{1,2})$, and therefore $z_{1,2} = 0$. $0 = \text{Tr}(y * (x^3 y^3) * z) = \text{Tr}(y * (x^3 y^3) * z_{2,1})$, and therefore $z_{2,1} = 0$. $0 = \text{Tr}((x^3 y^3) * z) = \text{Tr}((x^3 y^3) * z_{2,2})$, and therefore $z_{2,2} = 0$.

Since $\text{Tr}(x * (x^3 y^3) * z^2) = 0$, $z_{3,1} = 0$, and since $\text{Tr}(y * (x^3 y^3) * z^2) = 0$, $z_{1,3} = 0$.

From here on the proof is similar to what we already did in the case of $x^i y^j = x^2 y^4$, to prove that $V \subseteq F[xy^4]x + F(xy^4)^k$ for some $1 \leq k \leq 4$. \square

COROLLARY 5.3. (1) *The maximal 5-central spaces containing 5-central sets of size 3 are then of dimension 6.*

(2) *The intersection between every two 5-central spaces containing x, y and some third element of the form $x^i y^j$ can be 2, 3 or 5. See Diagram 1 for the spaces and their intersections.*

- (3) A 5-central space V of dimension greater or equal to 4 which contains a 5-central set of size 3 is contained in 4 different p -central spaces of degree 6 if and only if $V \subseteq F[z]w + Fz$ for some w and z satisfying $zw = \rho^k wz$ for some integer k . Otherwise, V is contained in exactly one 6 dimensional p -central space.

6. 3-Central Spaces spanned by 3-Central Sets

Let A be a central simple algebra over an infinite field F of characteristic not 3 containing a primitive 3rd root of unity ρ .

Let \mathcal{X} be the set of all 3-central elements in A . We build a directed graph (\mathcal{X}, E) by drawing an edge from y to x

$$y \longrightarrow x$$

if $xyy^{-1} = \rho x$. For any subset $B \subset \mathcal{X}$, (B, E_B) is the subgraph obtained by taking the vertices in B and all the edges between them.

REMARK 6.1. If $\{x, y\}$ is a 3-central set spanning a 3-central space then either $x \longrightarrow y$ or $x \longleftarrow y$.

PROOF. If $xy = yx$ then $x^2 * y = 3x^2y \in F$ which means that $y \in Fx$, contradiction. \square

According to [CV12, Corollary 2.2], a set $\{x_1, \dots, x_m\}$ spans a 3-central space if and only if every subset of cardinality three $\{x_i, x_j, x_k\}$ spans a 3-central space. Therefore we will start with the set of cardinality 3.

LEMMA 6.2. Given a 3-central set $\{x, y, z\}$, $Fx + Fy + Fz$ is 3-central if and only if (up to some permutation on $\{x, y, z\}$) either

$$\begin{array}{ccc} x & \longrightarrow & y \\ \downarrow & \nearrow & \\ z & & \end{array}$$

or $xyz \in F$, in which case

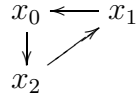
$$\begin{array}{ccc} x & \longleftarrow & y \\ \downarrow & \nearrow & \\ z & & \end{array}$$

PROOF. From Remark 6.1, the only possible graphs (up to permutation of the vertices) are the two graphs above. In the first case, $x * y * z = 0$, so there are no extra conditions. In the second case,

$x * y * z = -3\rho^{-1}xyz \in F$. The opposite direction is a straight-forward computation. \square

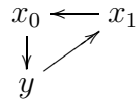
Let B be a 3-central set spanning a 3-central space. We will now study the properties of the directed graph (B, E_B) . By a cycle we always mean a **simple directed cycle**.

PROPOSITION 6.3. *If (B, E_B) contains a cycle of length 3*



then for every $y \in B \setminus \{x_0, x_1, x_2\}$, either $x_k \longrightarrow y$ for any $k \in \{0, 1, 2\}$ or $x_k \longleftarrow y$ for any $k \in \{0, 1, 2\}$.

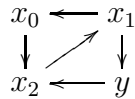
PROOF. If $x_0 \longrightarrow y$ and $x_1 \longleftarrow y$ then



which means that $yx_0x_1 \in F$. Since $x_0x_1x_2 \in F$, we get $y \in Fx_2$, which contradicts the linear independence. The rest of the proof repeats the same idea. \square

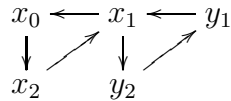
PROPOSITION 6.4. *The cycles of (B, E_B) are vertex-disjoint.*

PROOF. First assume that

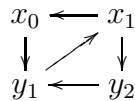


Then $yx_1x_2 \in F$ whereas $x_0x_1x_2 \in F$, which means that $y \in Fx_0$, and that contradicts the linear independence.

Assume that



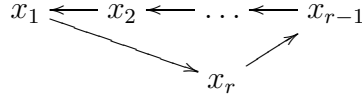
From Proposition 6.3 we have $x_0 \longrightarrow y_2$ and $y_1 \longrightarrow x_0$. But then



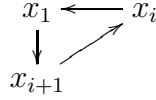
and we saw already that this is impossible. \square

PROPOSITION 6.5. *There are no cycles of length greater than 3.*

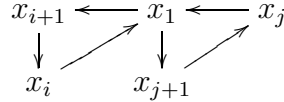
PROOF. Assume



for some $r \geq 4$. Let i be the maximal integer between 1 and r such that $x_i \longrightarrow x_1$. Now, $x_1 \longrightarrow x_{i+1}$. Therefore



If $i \geq 3$ then according to Proposition 6.3, $x_1 \longrightarrow x_{i-1}$, which implies that $i \neq 3$, or in other words $i \geq 4$. Let j be the minimal index for which $x_1 \longrightarrow x_{j+1}$. In particular $x_j \longrightarrow x_1$. Now, $j+1 \leq i-1$, which means that



But this is impossible. If $i = 2$ then according to Proposition 6.3, $x_4 \longrightarrow x_1$ which contradicts the maximality of i . \square

As a consequence we obtain the following theorem:

THEOREM 6.6. *A 3-central subset B of \mathcal{X} spans a 3-central space if and only if the graph (B, E_B) satisfies the following axioms:*

- (1) *For every two distinct elements $x, y \in B$, either $x \longrightarrow y$ or $x \longleftarrow y$*
- (2) *All cycles are of length 3.*
- (3) *The product of all the elements in a cycle is in F .*
- (4) *The cycles are vertex-disjoint.*

PROOF. The straight-forward direction is an immediate result of what we did so far. The opposite direction is a result of the fact that every three elements in this set span a 3-central space according to Lemma 6.2. \square

The following remark may help the reader get an idea of how the graph $(B, E(B))$ looks like:

REMARK 6.7. *Assume B is a 3-central set spanning a 3-central space. Let \sim be the following equivalence relation: $x \sim y$ if and only if $x = y$ or x and y belong to the same cycle in (B, E_B) . As we already saw, this equivalence relation is also direction preserving in the sense that*

if $x \longrightarrow z$ and $x \sim y$ then $y \longrightarrow z$ and if $z \longrightarrow x$ and $x \sim y$ then $z \longrightarrow y$. Define an order \leq on the equivalence classes: $[x] \leq [z]$ if $[x] = [z]$ or $z \longrightarrow x$. Then the set of equivalence classes is a fully ordered set.

One can therefore visualize the graph as graded into levels, where in each level we have either one element or a cycle, and each element has edges going from it to all the elements in the lower levels.

COROLLARY 6.8. *Given a 3-central set B spanning a 3-central space, if $\#B = m$ then the longest path $x_1 \longrightarrow x_2 \longrightarrow \dots \longrightarrow x_r$ in the graph (B, E_B) satisfying $x_i \longrightarrow x_j$ for any $1 \leq i < j \leq r$ is of length no less than $m - \lfloor \frac{m}{3} \rfloor$.*

PROOF. Take B and take off exactly one element from each cycle. The number of elements taken off is at most $\lfloor \frac{m}{3} \rfloor$, and what is left satisfies the required condition. \square

COROLLARY 6.9. *The maximal 3-central set spanning a 3-central space in A is of cardinality $3n + 1$.*

PROOF. We are already familiar with 3-central spaces spanned by 3-central sets of size $3n + 1$. According to the previous corollary, if we have a p -central set B of size $3n + 2$ spanning a 3-central space then we have a path in (B, E_B)

$$x_1 \longrightarrow x_2 \longrightarrow \dots \longrightarrow x_{2n+2}$$

satisfying $x_i \longrightarrow x_j$ for any $1 \leq i < j \leq 2n + 2$. Then the set B generates over F a tensor product of $n + 1$ cyclic algebras of degree 3

$$F[x_1, x_2] \otimes F[x_1 x_2^{-1} x_3, x_1 x_2^{-1} x_4] \otimes \dots \otimes F\left[\left(\prod_{k=1}^n x_{2k-1} x_{2k}^{-1}\right) x_{2n+1}, \left(\prod_{k=1}^n x_{2k-1} x_{2k}^{-1}\right) x_{2n+2}\right],$$

contradiction. \square

7. Algebras of Fixed Degrees with 3-Central Subspaces

In this section we study the effect of the existence of 3-central spaces in algebras of fixed degrees. We focus on degree 3. We show that for a field extension K/F , if a central simple K -algebra A of degree 3 contains an F -vector subspace V such that $v^3 \in F$ for all $v \in V$ and $[V : F] = 3$ then A is a restriction of a central simple F -algebra. We provide a counterexample in case $[V : F] = 2$.

7.1. Dimension 3.

LEMMA 7.1. *If a simple (noncentral) F -algebra contains a 3-dimensional F -vector subspace with third powers in F then it is a restriction of a central simple F -algebra.*

PROOF. From [Rac09] it is known that the F -vector space with third powers in F contains two elements ξ and μ such that $\xi\mu = \rho\mu\xi$. Consequently the algebra is a restriction of $F[\xi, \mu]$ which is a cyclic algebra of degree 3 over F . \square

7.2. Dimension 2. Let K/F be an extension of dimension 3, with a third root of unity $\rho \in F$. Let $\alpha \in F^\times$ and $b \in K^\times$.

LEMMA 7.2. *A division F -algebra D contains a 3-central space $Fx + Fy$ such that $x^3 = \alpha$, $y^3 = \beta$, $x^2 * y = 0$ and $x * y^2 = 3\delta$ iff there exists an element u such that $xu = \rho ux$ and $\frac{\beta-b}{\alpha b^2} + \frac{\delta^3}{\alpha^2 b^3}$ has a cubic root in $F[b]$ where $b = u^3$.*

PROOF. (\Rightarrow) According to [Hai84], there exists an element u for which $xu = \rho ux$ and $y = u + a_1 u^2 x + \frac{3\delta}{\alpha b(\rho-1)^2} u^2 x^2$ where $a_1 \in \text{cent}(F[x, u]) = F[b]$. $y^3 = b + a_1^3 \alpha b^2 + \frac{27\delta^3}{\alpha^3 b^3 (\rho-1)^6} \alpha^2 b^2 = \beta$, hence $a_1^3 = \frac{\beta-b}{\alpha b^2} + \frac{\delta^3}{\alpha^2 b^3}$.

(\Leftarrow) If indeed $\frac{\beta-b}{\alpha b^2} + \frac{\delta^3}{\alpha^2 b^3}$ has a cubic root in $F[b]$ then it can be denoted by a_1 , and so the element $y = u + a_1 u^2 x + \frac{3\delta}{\alpha b(\rho-1)^2} u^2 x^2$ satisfies $y^3 = \beta$, $x^2 * y = 0$ and $x * y^2 = \delta$. \square

REMARK 7.3. *The standard generator x in the cyclic algebra $A = (\alpha, b)_K$ extends to a 2-dimensional 3-central space (with $\gamma = 0$ and δ as in Lemma 7.2) over F iff*

$$(\delta^3 + \alpha\beta b - \alpha b^2)\alpha$$

is a third power in K for a suitable $\beta \in F$.

PROOF. The same proof as in Lemma 7.2. Mind that $(\delta^3 + \alpha\beta b - \alpha b^2)\alpha = (\frac{\beta-b}{\alpha b^2} + \frac{\delta^3}{\alpha^2 b^3})\alpha^3 b^3$. \square

REMARK 7.4. *We may assume $\delta = 0$ (orthogonal space) or $\delta = 1$ (non-orthogonal).*

Namely, for some $d \in K$, $(\delta^3 + \alpha\beta b - \alpha b^2)\alpha = -d^3$. Let $\theta = \frac{\alpha\beta}{2}$, and put $b = \frac{1}{\alpha}c + \frac{1}{2}\beta$ for $c \in K$: the equation becomes

$$(28) \quad c^2 = d^3 + \delta^3 \alpha + \theta^2.$$

Fact. Let $c \in K$ and $\theta \in F$. Fx extends to a 2-dimensional 3-central space over F in $(\alpha, c + \theta) = K[x, y]$ iff for some $\delta \in F$ and $d \in K$, (28) holds.

THEOREM 7.5. *Let k be a field with third root of unity, and let $\delta \in k$. There exist:*

- a field F containing k
- with a cubic Galois extension K/F
- and a cyclic algebra A of degree 3 over K ,

such that A admits a 2-dimensional 3-central F -space of type δ , and $\text{cor}_{K/F}A$ is non-trivial. In particular A is not restricted from F .

The proof occupies the rest of this section.

LEMMA 7.6. *Suppose K has commuting automorphisms τ_0, τ_1, τ_2 of order 2 and an automorphism σ of order 3, such that $\sigma\tau_\ell\sigma^{-1} = \tau_{\ell+1 \pmod{3}}$. Let $F_0 = K^{\tau_0, \tau_1, \tau_2, \sigma}$. Let $\alpha, \delta, \theta \in F_0$. Suppose $d \in K_0 = K^{\tau_0, \tau_1, \tau_2}$. Suppose $c \in K$ is an element such that $\tau_\ell\sigma^{\ell'}(c) = (-1)^{\delta_{\ell, \ell'}}\sigma^{\ell'}(c)$, where Kronecker's delta applies to ℓ and ℓ' modulo 3. Assume $c^2 = d^3 + \delta^3\alpha + \theta^2$.*

If $A = (\alpha, c + \theta)_K$ is not split, then its corestriction to F is not split as well.

PROOF. Write $c_\ell = \sigma^\ell c$ and $d_\ell = \sigma^\ell(d)$. By the projection formula, the corestriction is $\text{cor}_{K/F}A = (\alpha, (c_0 + \theta)(c_1 + \theta)(c_2 + \theta))_F$. We may assume α is not a cube in K , so let $\tilde{K} = K[x : x^3 = \alpha]$, with the action of $\text{Gal}(K/F_0)$ extended by acting trivially on x , and let $\tilde{F} = \tilde{K}^\sigma$.

Suppose

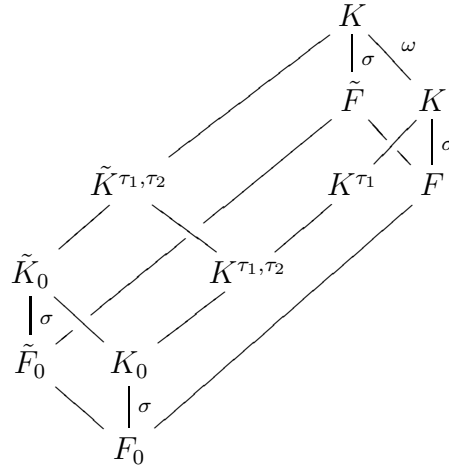
$$(c_0 + \theta)(c_1 + \theta)(c_2 + \theta) = N_{\tilde{K}/\tilde{F}}(f)$$

for some $f \in \tilde{F}$. By assumption $\alpha \in F_0$, so the τ_ℓ commute with the elements of $\text{Gal}(\tilde{K}/\tilde{F})$. Taking the norm with respect to τ_1 and τ_2 , we get

$$(c_0 + \theta)^4(c_1^2 - \theta^2)(c_2^2 - \theta^2)^2 = N_\omega(N_{\tau_1}N_{\tau_2}f);$$

notice that the τ_ℓ do not act on \tilde{F} , so the most we can say is that $N_{\tau_1}N_{\tau_2}f \in \tilde{K}^{\tau_1, \tau_2}$.

But $c_\ell^2 - \theta^2 = d^3 + \delta^3\alpha = N_{\tilde{K}/\tilde{F}}(d_\ell + \delta x)$, with $d_\ell + \delta x \in \tilde{K}_0$; so $(c_0 + \theta)^4$, and therefore $c_0 + \theta$, are norms in the extension $\tilde{K}^{\tau_1, \tau_2}/K^{\tau_1, \tau_2}$. This proves that the algebra $A_0 = (\alpha, c_0 + \theta)_{K^{\tau_1, \tau_2}}$ is split, and so $A = A_0 \otimes_{K^{\tau_1, \tau_2}} K$ is split as well. \square



Let us realize the construction of Lemma 7.6. Let k be a field with 3rd root of unity $\rho \in k$, and let $\delta \in k$ be arbitrary, but fixed (eventually we take $\delta = 0$ or $\delta = 1$). Let \tilde{K}_0 be the transcendental extension $\tilde{K}_0 = k(x, \theta, d_0, d_1, d_2)$, and set $\alpha = x^3$. Let \tilde{K} be the field extension $\tilde{K}_0[c_0, c_1, c_2]$, subject to the relations

$$c_\ell^2 = d_\ell^3 + (\delta^3 \alpha + \theta^2)$$

for $\ell = 0, 1, 2$. Clearly $[\tilde{K} : \tilde{K}_0] = 8$. Define an automorphism σ of \tilde{K} by fixing x and θ , and permuting the d_ℓ and c_ℓ cyclically. Then let $\tilde{F} = \tilde{K}^\sigma$ and $\tilde{F}_0 = \tilde{K}_0^\sigma$. Note that $\text{Gal}(\tilde{K}/\tilde{F}_0)$ is a wreath product $\mathbb{Z}_2 \wr \mathbb{Z}_3$; \tilde{K}_0 is Galois over \tilde{F}_0 , but \tilde{F} is not.

Let ω be the automorphism of \tilde{K} defined by $\omega(x) = \rho x$ and fixing all other generators. Let $K = \tilde{K}^\omega$ and similarly $F = \tilde{F}^\omega$, $K_0 = \tilde{K}_0^\omega$ and $F_0 = \tilde{F}_0^\omega$. Since ω commutes with $\text{Gal}(\tilde{K}/\tilde{K}_0)$, we have that $\tilde{K} = \tilde{K}_0 \otimes_{F_0} K$.

We take K/F to be the field extension asserted in the theorem, with the algebra $A = (\alpha, c_0 + \theta)_K$. It remains to prove that A is a division algebra. This may seem obvious, as the construction is fairly generic, but (28) imposes a severe restriction — implying, in fact, that $N_{\tau_0}(c + \theta)$ is a norm in \tilde{K}/K , so $\text{cor}_{K/K^{\tau_0}} A$ is split.

Take $c = c_0$ and $d = d_0$, so (28) is solved. Then $N_{K/F}(c + \theta) = (c_0 + \theta)(c_1 + \theta)(c_2 + \theta)$, which is clearly in F . We need to show that this element is not a norm in \tilde{F}/F .

Let $\tau_0, \tau_1, \tau_2 \in \text{Gal}(K/K_0)$ be defined by $\tau_i(c_i) = -c_i$ and $\tau_i(c_j) = c_j$ for $j \neq i$.

Suppose

$$(29) \quad c_0 + \theta = N_\omega(h)$$

for some $h \in \tilde{K}^{\tau_1, \tau_2} = \tilde{K}_0[c_0]$. Let $k' = k(d_1, d_2)$. So we need to prove that $c_0 + \theta$ is not a norm from $k'(\theta, x, d_0)[c_0]$ to $k'(\theta, \alpha, d_0)[c_0]$.

LEMMA 7.7. *Let k' be any field of characteristic not 2 or 3, and let c be defined by (28). The element $c + \theta$ is not a norm in the extension $k(\theta, x, d)[c]/k(\theta, x^3, d)[c]$, where $c^2 = d^3 + \delta^3 x^3 + \theta^2$.*

PROOF. Indeed, write $h = h_2^{-1}(h_0 + h_1 c)$ for $h_0, h_1, h_2 \in k[x, \theta, d_0]$. Then $N_\omega(h_2)(c + \theta) = N_\omega(h_0 + h_1 c)$, which are the equations in Lemma 7.8 below, showing that $h_2 = 0$ contrary to assumption. \square

LEMMA 7.8. *Let $h_0, h_1, h_2 \in k[\theta, x, d_0]$ be polynomials satisfying*

$$(30) \quad N_\omega(h_2) = \text{Tr}_\omega(h_0 \omega(h_0) \omega^2(h_1)) + N_\omega(h_1)(\delta^3 x^3 + \theta^2)$$

$$(31) \quad \theta N_\omega(h_2) = N_\omega(h_0) + \text{Tr}_\omega(h_1 \omega(h_1) \omega^2(h_0))(\delta^3 x^3 + \theta^2),$$

where ω is the automorphism defined above. Then $h_0, h_1, h_2 = 0$.

PROOF. Since for every $f \in k[\theta, x, d_0]$ we have that $\omega(f) \equiv f \pmod{x}$ and $N_\omega(f) \equiv f^3$, reduction modulo x gives

$$(32) \quad \bar{h}_2^3 = 3\bar{h}_0^2 \bar{h}_1 + (d_0^3 + \theta^2) \bar{h}_1^3$$

$$(33) \quad \theta \bar{h}_2^3 = \bar{h}_0^3 + 3(d_0^3 + \theta^2) \bar{h}_0 \bar{h}_1^2$$

for the residues $\bar{h}_0, \bar{h}_1, \bar{h}_2 \in k[\theta, d_0]$. But then $(\bar{h}_0 - \theta \bar{h}_1)^3 = \bar{h}_0^3 - 3\theta \bar{h}_1 \bar{h}_0^2 + 3\theta^2 \bar{h}_0 \bar{h}_1^2 - \theta^3 \bar{h}_1^3 = (\theta \bar{h}_2^3 - 3d_0^3 \bar{h}_0 \bar{h}_1^2) - (\theta \bar{h}_2^3 - \theta d_0^3 \bar{h}_1^3) = (\theta \bar{h}_1 - 3\bar{h}_0) d_0^3 \bar{h}_1^2$, namely

$$(34) \quad (\bar{h}_0 - \theta \bar{h}_1)^3 = (\theta \bar{h}_1 - 3\bar{h}_0) d_0^3 \bar{h}_1^2.$$

This implies $\bar{h}_0 \equiv \theta \bar{h}_1 \pmod{d_0}$, so we can write $\bar{h}_0 = \theta \bar{h}_1 + d_0 \bar{h}'_0$ for $\bar{h}'_0 \in k[\theta, d_0]$. Plugging this back in (34) and dividing by d_0^3 , we get

$$\bar{h}'_0^3 + 3d_0 \bar{h}'_0 \bar{h}_1^2 + 2\theta \bar{h}_1^3 = 0,$$

which by Lemma 7.9 implies that $\bar{h}'_0 = 0$. Thus $\bar{h}_0 = \theta \bar{h}_1$, and (32) gives

$$\bar{h}_2^3 = (d_0^3 + \theta^2 + 3\theta) \bar{h}_1^3.$$

But $d_0^3 + \theta^2 + 3\theta$ is not a cube in $k(\theta, d_0)$, so necessarily $\bar{h}_1 = \bar{h}_2 = 0$, implying $\bar{h}_0 = 0$ as well. This proves h_0, h_1, h_2 are all divisible by x , so replacing each h_ℓ by $x^{-1} h_\ell$ we get a solution of smaller degree to (30)–(31), ad infinitum. \square

LEMMA 7.9. *If $f, g \in k[\theta, d_0]$ satisfy*

$$f^3 + 3d_0fg^2 + 2\theta g^3 = 0$$

then $f = 0$.

PROOF. Otherwise $f^{-1}g$ is a root of $\lambda^3 + 3d_0\lambda + 2\theta$, which is generic over $k(\theta, d_0)$ since $\text{char } k \neq 2, 3$, and thus irreducible. \square

CHAPTER 3

Chain Lemmas

1. Background

It was proven by Merkurjev and Suslin in [MS82] that the group ${}_dBr(F)$ (the d -torsion of $Br(F)$) is generated by cyclic algebras of degree d for any integer d , if F is a field of characteristic prime to d containing a primitive d th root of unity.

It had been proven earlier by Albert in [Alb61] that ${}_pBr(F)$ is generated by cyclic algebras of degree p if F is a field of characteristic p .

The word problem for ${}_dBr(F)$ can be phrased in terms of tensor products of cyclic algebras: Are two given two tensor products of cyclic algebras Brauer equivalent?

Given two tensor products of cyclic algebras, if they are not of the same length then one can add a matrix algebra to the shorter side and make them have the same length. In this case, being Brauer equivalent is the same as being isomorphic as central simple F -algebras.

Two different symbols might present the same algebra. For example, the real quaternion algebra is presented by both $(-1, -1)_{2, \mathbb{R}}$ and $(-1, -2)_{2, \mathbb{R}}$.

Of course, two different tensor products of cyclic algebras might present the same algebra even if the multiplicands are not pair-wise isomorphic. For example, $(-1, -1)_{2, \mathbb{R}} \otimes (-1, -1)_{2, \mathbb{R}} = (1, 1)_{2, \mathbb{R}} \otimes (1, 1)_{2, \mathbb{R}}$, even though $(-1, -1)_{2, \mathbb{R}}$ is a division algebra while $(1, 1)_{2, \mathbb{R}}$ is a matrix algebra (and in particular they are not isomorphic).

The idea of the chain lemma is to come up with a set of basic steps with which one can produce of the different symbol presentations of an algebra as tensor products of cyclic algebras, given one symbol presentations to start with.

So far there are known chain lemmas for quaternion algebras, bi-quaternion algebras (see Section 3) and cyclic algebras of degree 3. The latter was proven in case of characteristic not 3 by Rost in [Ros99] and in case of characteristic 3 by Vishne in [Vis02]. In [HKT09], Haile

Kuo and Tignol provided alternative proofs for Rost's result, using composition algebras.

2. Chains of p -Central Elements in p -Cyclic Algebras

Throughout this section, let p be a given prime and F be an infinite field.

We consider always one of the two cases:

- (1) $\text{char}(F) = p$.
- (2) $\text{char}(F) \neq p$ and F contains a primitive p th root of unity ρ .

In this section, we focus mainly on Case 2 (except for Subsection 2.3). Instead of asking whether two symbol presentations of the same cyclic algebra are connected by a chain of basic steps, we ask whether two given p -central elements x and z are connected by a chain of p -central elements $x = x_1, x_2, \dots, x_n = z$ such that $x_k x_{k+1} = \rho^{d_k} x_{k+1} x_k$ for any $1 \leq k \leq n-1$ and a set of integers $\{d_k\}$.

The technique. Let A be a cyclic algebra of degree p over F in Case 2.

If $x \in A$ is p -central, then one can decompose A under the conjugation action of x into $A = \sum_{i=0}^{p-1} A_i$, where A_i is the eigenspace for the eigenvalue ρ^i . In particular, if we have two p -central elements x and z , then $z = z_0 + \dots + z_{p-1}$ such that $z_i x = \rho^i x z_i$ and $x = x_0 + \dots + x_{p-1}$ where $x_i z = \rho^i z x_i$. The indices can be considered to be elements in $\mathbb{Z}/p\mathbb{Z}$.

We recall that a p -central space $Fx + Fz$ is short of type $\{i, j\}$ if $z = z_i + z_j$.

Let \mathcal{X} be the set of p -central elements, and let $E = \mathcal{X} \times \mathcal{X}$. The pair (\mathcal{X}, E) forms a complete directed graph. We label each edge $(x, z) \in E$ with the set $\{i \in \mathbb{Z}/p\mathbb{Z} : z_i \neq 0\}$ and denote it by $l(x, z)$. The weight of each edge is then $\sharp l(x, z)$ and is denoted by $w(x, z)$.

When drawing an edge, we can either write the label explicitly $x \xrightarrow{\{a_1, \dots, a_k\}} z$, or simply mention its weight $x \xrightarrow{k} z$. If we want to describe the label of each direction, then we shall write the label of the direction from left to right above the edge and the label of the direction from right to left below the edge $x \xleftrightarrow[\{b_1, \dots, b_m\}]{\{a_1, \dots, a_k\}} z$. The same

goes for weights $x \xleftrightarrow[m]{k} z$. When $w(x, z) = 1$ then also $w(z, x) = 1$, and therefore we shall simply draw $x \longleftrightarrow z$.

REMARK 2.1. *It is not true in general that $w(x, z) = w(z, x)$, except for the trivial case of $w(x, z) = 1$. For example, if $p = 3$ and $A = (\alpha, \beta)_{3,F} = F[x, y : x^3 = \alpha, y^3 = \beta, yx = \rho xy]$ then for $z = y + x^2y^2$ we have $x = (-\rho\beta\alpha - \rho^2\alpha^{-1})(z - x^2yz - (\rho^2\alpha^2\beta)^{-1}(x^2y)^2z)$. In this case, $x_0 = (-\rho\beta\alpha - \rho^2\alpha^{-1})z$, $x_1 = (-\rho\beta\alpha - \rho^2\alpha^{-1})(-x^2y)$ and $x_2 = (-\rho\beta\alpha - \rho^2\alpha^{-1})(-\rho^2\alpha^2\beta)^{-1}(x^2y)^2z$. Consequently, $w(x, z) = 2 \neq 3 = w(z, x)$.*

DEFINITION 2.2. *We call a chain of edges of weight 1 a “Rost chain”.*

Subsection 2.1 focuses on edges of weight 2 in both directions. The main result in that section is

Theorem 2.11 If $x \xleftrightarrow{2} z$ then there exists a Rost chain connecting x and z of length 2.

Subsection 2.2 is dedicated to showing how the chain lemma for the case of $p = 3$ is obtained as a result of more general statements that hold for any arbitrary prime p .

Subsection 2.3 provides a better upper bound for the distance between two Artin-Schreier elements than what appears in [MV14].

Subsection 2.4 deals with the special case of $p = 5$. The main result in that section is

Theorem 2.26 If $x \xrightarrow{2} z$, and $0 \notin l(z, x)$ then there is a Rost chain connecting x and z .

DEFINITION 2.3. *The commutator $[x, z]_d$ has a different meaning in each case.*

In Case 1, we write $[x, z] = [x, z]_1 = zx - xz$ and define $[x, z]_k$ inductively as $[x, z]_{k-1}x - x[x, z]_{k-1}$. $[x, z]_0$ is defined to be z .

In Case 2, $[x, z]_d = zx - \rho^d xz$. We define inductively inductively:

$$[x, \dots, x, x, z]_{d_1, d_2, \dots, d_k} = [x, \dots, x, [x, z]_{d_1}]_{d_2, \dots, d_k}.$$

REMARK 2.4. *In Case 2, $[x, \dots, x, z]_{d_1, d_2, \dots, d_k} = 0$ if and only if $l(x, z) \subseteq \{d_1, d_2, \dots, d_k\}$*

PROOF. Straightforward calculation shows that the part of $[x, \dots, x, z]_{d_1, d_2, \dots, d_k}$ which acts on x with ρ^i is $(\rho^i - \rho^{d_1}) \dots (\rho^i - \rho^{d_k}) x^k z_i$. This is equal to zero if and only if $i \in \{d_1, d_2, \dots, d_k\}$. \square

2.1. Edge of weight 2 in both directions. In this section we study some basic properties of the graph (\mathcal{X}, E) in attempt to prove that if $w(x, z) = w(z, x) = 2$ then x and z are connected by a Rost chain of length 2.

PROPOSITION 2.5. If $x \xleftrightarrow{2} z$ then

- (1) $l(z, x) = -l(x, z)$, i.e. $x = x_i + x_j$ and $z = z_{-i} + z_{-j}$ for some $i \neq j$.
- (2) $x_i x_j = \rho^{j-i} x_j x_i$ and $z_{-i} z_{-j} = \rho^{i-j} z_{-j} z_{-i}$.

PROOF. We have $x = x_i + x_j$ and $z = z_m + z_n$ such that $z_m x = \rho^m x z_m$, $z_n x = \rho^n x z_n$, $x_i z = \rho^i z x_i$ and $x_j z = \rho^j z x_j$.

Let us consider the equality $[x, x, z]_{m,n} = 0$. This holds because $z = z_m + z_n$. On the other hand, if we substitute $x = x_i + x_j$ in this expression we get the following set of equations (due to conjugation by z):

- (1) $(zx_i - \rho^m x_i z)x_i - \rho^n x_i(zx_i - \rho^m x_i z) = 0$
- (2) $(zx_j - \rho^m x_j z)x_j - \rho^n x_j(zx_j - \rho^m x_j z) = 0$
- (3) $(zx_j - \rho^m x_j z)x_i - \rho^n x_i(zx_j - \rho^m x_j z) + (zx_i - \rho^m x_i z)x_j - \rho^n x_j(zx_i - \rho^m x_i z) = 0$

From the first equation we obtain $(\rho^{-i} - \rho^m)(\rho^{-i} - \rho^n)x_i^2 z = 0$ and from the second equation we obtain $(\rho^{-j} - \rho^m)(\rho^{-j} - \rho^n)x_j^2 z = 0$. Henceforth, without loss of generality $m = -i$ and $n = -j$.

From the third equation we obtain $(\rho^{-j} - \rho^{-i})\rho^{-i}x_j x_i z - (\rho^{-j} - \rho^{-i})\rho^{-j}x_i x_j z = 0$. Consequently, $x_i x_j = \rho^{j-i} x_j x_i$. Due to symmetry, we also have $z_{-i} z_{-j} = \rho^{i-j} z_{-j} z_{-i}$. \square

COROLLARY 2.6. For any $x, z \in \mathcal{X}$, $x \xleftrightarrow{2} z$ if and only if $z \in Fy^i + Fy^j x^{(j-i)i^{-1}}$ for some $y \in \mathcal{X}$ satisfying $yx = \rho xy$.

PROOF. If $x \xleftrightarrow{2} z$ then $z \in Fy^i + Fy^j x^{(j-i)i^{-1}}$ according to Proposition 2.5.

In order to prove the opposite direction it is enough to check what happens if $i = 1$, i.e. check whether $w(z, x) = 2$ if $z = y + y^d x^{d-1}$ for some $y \in \mathcal{X}$ satisfying $yx = \rho xy$. This is true, because $[x, x, z]_{d,1} = 0$. \square

REMARK 2.7. If $0 \neq k \in l(x, z)$ then $z_k \in \mathcal{X}$. However, if $0 \in l(x, z)$ then z_0 is not necessarily in \mathcal{X} . For example: If $p = 3$ and $A = F[x, y : x^3 = \alpha, y^3 = \beta, yx = \rho xy]$ then $z = x + x^2 + xy - \frac{1}{\beta}(xy)^2$ satisfies $\text{Tr}(z) = \text{Tr}(z^2) = 0$, and so $z^3 \in F$, i.e. $z \in \mathcal{X}$, even though $z_0 = x + x^2 \notin \mathcal{X}$.

PROPOSITION 2.8. If $x \xrightarrow{\{i,j\}} z$, then $z_i, z_j \in \mathcal{X}$.

PROOF. We have $F \ni z^p = (z_i + z_j)^p = \sum_{k=0}^p z_i^k * z_j^{p-k}$. There is a unique decomposition into eigenvectors with respect to conjugation by x . Since the left-hand side of the equality commutes with x , it must be equal to the part of the right-hand side of this equality which commutes with x . Therefore $z^p = z_i^p + z_j^p$. If $i \neq 0$ then $F[x, z_i]$ generates a subalgebra of A whose center is $F[z_i^p]$. However, this subalgebra is noncommutative, and as a cyclic division algebra of prime degree, A has no nontrivial noncommutative subalgebras, which means that $A = F[x, z_i]$ and in particular, $z_i^p \in F$. Similarly, if $j \neq 0$ then $z_j^p \in F$. If $i = 0$ then $j \neq 0$ and so $z_j \in \mathcal{X}$, and consequently $z_i^p = z^p - z_j^p \in F$, which means that $z_i \in \mathcal{X}$. \square

COROLLARY 2.9. If $x \xrightarrow{\{i,j\}} z$ then $Fz_i + Fz_j$ is a p -central space. Moreover, its exponentiation form $f(u, v) = (uz_i + vz_j)^p$ is diagonal, i.e. $f(u, z) = u^p z_i^p + v^p z_j^p$.

PROOF. We have $z^p = (z_i + z_j)^p$. Due to conjugation by x we obtain the relations $z_i^k * z_j^{p-k} = 0$ for all $1 \leq k \leq p-1$. Together with the result from Proposition 2.8, the space $Fz_i + Fz_j$ is therefore p -central and it is easy to see why the exponentiation form is diagonal. \square

COROLLARY 2.10. If $x \xrightarrow{\{i,j\}} z$ then $0 \notin l(z_i, z_j)$, and in particular $w(z_i, z_j) \leq p-1$.

PROOF. The exponentiation form of $Fz_i + Fz_j$ is diagonal, therefore $z_i^{p-1} * z_j = 0$. However, $z_i^{p-1} * z_j = pz_i^{p-1}z_{j,0}$, which means that $z_{j,0} = 0$. \square

THEOREM 2.11. If $x \xleftrightarrow{2} z$ then there exists a Rost chain connecting x and z of length 2.

PROOF. We have $x = x_i + x_j$ and $z = z_{-i} + z_{-j}$ according to Proposition 2.5. Setting $y = xz - \rho^i z x$ we have $y = (\rho^j - \rho^i)z x_j$. Therefore $y^p = (\rho^j - \rho^i)^p z^p x_j^p$. According to Proposition 2.8 we know that $x_j \in \mathcal{X}$, and therefore $y \in \mathcal{X}$. Since $w(x, y) = w(z, y) = 1$ we get the Rost chain $x \longleftrightarrow y \longleftrightarrow z$. \square

2.2. Alternative proofs for the Chain Lemma for $p = 3$. In this section we show how the chain lemma for $p = 3$ is easily obtained as a result of more general statements that hold for any prime p .

REMARK 2.12. If $x \xrightarrow{\{i,j\}} z$ and $z_i \longleftrightarrow z_j$ then $x \longleftrightarrow z_i z_j^{-1} \longleftrightarrow z$.

COROLLARY 2.13. If $x \xrightarrow{\{0,j\}} z$ then $z_0 \longleftrightarrow z_j$. Moreover, there exists a Rost chain between x and z of length 2.

PROOF. Since A is cyclic of degree p , and $z_0 \in \mathcal{X}$ (according to 2.8), $z_0 = x^k$ for some k . Henceforth $w(z_0, z_j) = 1$. As a Result of Remark 2.12, there is a Rost chain between x and z of length 2. \square

PROPOSITION 2.14. If $x \xrightarrow{\{i,j\}} z$ and $z_i \xrightarrow{\{m,n\}} z_j$ then $m \not\equiv -n \pmod{p}$.

PROOF. According to Corollary 2.13, $i \neq 0$ because $w(z_i, z_j) = 2$. Therefore $z_{j,m} \in Fz_i^{j^{i-1}} x^{m(-i)^{-1}}$ and $z_{j,n} \in Fz_i^{j^{i-1}} x^{n(-i)^{-1}}$.

We have $m, n \neq 0$ due to Corollary 2.10.

On the contrary, let us assume that $m \equiv -n \pmod{p}$.

In Corollary 2.9 we saw that $Fz_i + Fz_j$ is a p -central space with a diagonal exponentiation form. Since $l(z_i, z_j) = \{m, -m\}$, this p -central space is short of type $\{m, -m\}$.

In [CV12] it was proven that if $Fr + Fs$ is a short p -central space of type $\{t, -t\}$ whose exponentiation form is diagonal then $s_t s_{-t} = \rho^t s_{-t} s_t$.

Therefore $z_{j,m} z_{j,n} = \rho^m z_{j,n} z_{j,m}$. Consequently $\rho^{i^{-2}j(m-n)} = \rho^m$, which means that $2j \equiv i^2 \pmod{p}$.

But now, $l(x^2, z) = \{2i, 2j\}$ and therefore for similar arguments $2(2j) \equiv (2i)^2 \pmod{p}$, and that is a contradiction. \square

PROPOSITION 2.15. If $l(x, z) \subseteq \{0, i, j\}$ and $l(z, x) \subseteq \{0, -i, k\}$ for some $i, j, k \in \mathbb{Z}/p\mathbb{Z}$, and $z_0 \in Fx^{-1} + Fx^m$ and $x_0 \in Fz^{-1} + Fz^n$ for some $n, m \in \mathbb{Z}$, then there is a Rost chain of length less or equal to 4 connecting x and z .

PROOF. From $l(x, z) \subseteq \{0, i, j\}$ we have $z = z_0 + z_i + z_j$ (some of them may be equal to zero). Similarly, $x = x_0 + x_{-i} + x_k$. Let $t = \frac{zx - \rho^i xz}{1 - \rho^i} - \text{Tr}(xz)$. By substituting the details given above, $t \in Fxz_j + Fx^{m+1}$. Consequently, $x \longleftrightarrow x^{-m} z_j \longleftrightarrow t$. For similar reasons, $t \longleftrightarrow z^{-n} x_k \longleftrightarrow z$. \square

REMARK 2.16. *This Proposition generalizes the algebraic proof of Rost's chain lemma as appears in [HKT09]. Simply, for $p = 3$ all the conditions appearing in this proposition are automatically satisfied: We have $l(x, z), l(z, x) \subseteq \{0, 1, 2\}$, and also $z_0 \in Fx + Fx^2$ (the coefficient of $x^0 = 1$ must be zero because $\text{Tr}(z) = 0$) and $x_0 \in Fz + Fz^2$ (for a similar reason).*

PROPOSITION 2.17. *For all $x, z \in \mathcal{X}$ and $i \in \mathbb{Z}/p\mathbb{Z}$, there exists an element $t \in \mathcal{X}$ such that there is a Rost chain between x and t , and $i \notin l(z, t)$.*

PROOF. Since $x \in \mathcal{X}$, there exists an element $y \in \mathcal{X}$ such that $yx = \rho xy$. The vector space $Fx + F[x]y$ is p -central of dimension $p + 1$ (over F). However, the dimension of $\{w \in A : zw = \rho^i wz\}$ is a vector space of dimension p over F . Therefore the equation $c_0 y_i + c_1 (xy)_i + \dots + c_{p-1} (x^{p-1}y)_i + c_p x_i = 0$ should have a non-trivial solution, where $y_i, \dots, (x^{p-1}y)_i, x_i$ are the parts of $y, \dots, (x^{p-1}y), x$ respectively which act on z with ρ^i . Consequently, there exists a nonzero element $t \in Fx + F[x]y$ so that $t_i = 0$, i.e. $i \notin l(z, t)$. Finally, $l(x, t) \subseteq \{0, p-1\}$, and so according to Corollary 2.13 there is a Rost chain between x and t . \square

REMARK 2.18. *Rost's chain lemma for $p = 3$ is an easy result of this proposition. If $x, z \in \mathcal{X}$ then there exists $t \in \mathcal{X}$ such that x and t are connected by a Rost chain and $2 \notin l(z, t)$. This means, however, that $l(z, t) \subseteq \{0, 1\}$ and so according to Corollary 2.13, z and t are also connected by a Rost chain.*

2.3. Cyclic algebras of degree 3 in Characteristic 3. Unlike the other sections, in this section we focus on Case 2, and specifically $p = 3$.

In [Vis02], Vishne proved that given a cyclic algebra of degree 3 over a field of characteristic 3, one can move from one symbol presentation of the algebra to another by a series of 7 steps, such that in each step one entry remains unchanged.

In [MV14], Matzri and Vishne proved that given two symbol presentations, $[\alpha, \beta)$ and $[\gamma, \delta)$, one can get from $[\alpha, \beta)$ to either $[\gamma, \delta)$ or to $[-\gamma, \delta^2)$ by a series of 5 steps.

Here we shall prove that one can move from $[\alpha, \beta)$ either to $[\gamma, \delta)$ in five steps or to $[-\gamma, \delta^2)$ in three steps.

Like the eigenvector decomposition of elements with respect to a given p -central element in Case 2, we have a similar decomposition of elements with respect to a given Artin-Schreier element in Case 1.

In this context, we write $[x, z] = [x, z]_1 = zx - xz$ and define $[x, z]_k$ inductively as $[x, z]_{k-1}x - x[x, z]_{k-1}$. $[x, z]_0$ is defined to be z .

LEMMA 2.19. *Given an associative algebra A over a field F of characteristic p , if x is Artin-Schreier then for any $z \in A$, $z = z_0 + z_1 + \cdots + z_{p-1}$ where $[x, z_k] = kz_k$.*

PROOF. Let $z_0 = z - [x, z]_{p-1}$, and for all $1 \leq k \leq p-1$, $z_k = -(k^{p-1}[x, z]_1 + \cdots + k[x, z]_{p-2} + [z, x]_{p-1})$. It is an easy calculation to prove that $[x, z] = kz_k$. It is obvious that $z_0 + z_1 + \cdots + z_{p-1} = z$. \square

Let A be a cyclic algebra of degree 3 over F of characteristic 3.

THEOREM 2.20. *If x and z are Artin-Schreier then*

- (1) *If one of the elements z_1, z_2, x_1, x_2 is zero then there exists some 3-central element q such that $xq + qx = q$ and either $zq + qz = q$ or $zq + qz = -q$.*
- (2) *If $z_1, z_2, x_1, x_2 \neq 0$ then there exists some Artin-Schreier element t and some 3-central elements q, r such that $xq - qx = q$, $tq - qt = q$, $tr - rt = r$ and $zr - rz = r$.*

PROOF. According to Lemma 2.19, $z = z_0 + z_1 + z_2$ with respect to x and $x = x_0 + x_1 + x_2$ with respect to z . Now, $z_0 = a + bx + cx^2$ for some $a, b, c \in F$. However, $0 = \text{Tr}(z) = \text{Tr}(z_0) = c$. Furthermore, $b = \text{Tr}(xz)$. Similarly, $x_0 = d + bz$.

If $z_2 = 0$ then $z = a + bx + z_1$. Since z is Artin-Schreier, by the fact that $z^3 - z \in F$ we conclude that b is either 1 or -1 .

If $z_1 \neq 0$ then take $q = z_1$. Otherwise, take $q = y$ where y satisfies $xy + yx = y$.

Assume $z_1, z_2, x_1, x_2 \neq 0$. Let $w = xz - zx + x + z$. On one hand $w = z_0 - z_1 + x = a + (b+1)x - z_1$. On the other $w = x_0 - x_2 + z = d + (b+1)z - x_2$.

The element w is Artin-Schreier if and only if $b \neq -1$. In this case, we will take $q = z_1$, $t = (b+1)^{-1}w$, $r = x_1$. \square

2.4. The special case of $p = 5$. Back to Case 2. The final goal of this section is to prove the following sufficient condition for the existence of a Rost chain connecting two elements for the case of $p = 5$: $w(x, z) = 2$ and $0 \notin l(z, x)$.

LEMMA 2.21. *If $x \xrightarrow{\{i,j,k\}} z$ then $(2i \equiv j+k \pmod{p}) \wedge (2j \equiv i+k \pmod{p})$ if and only if $p = 3$.*

PROOF. If $2i \equiv j + k \pmod{p}$ and $2j \equiv i + k \pmod{p}$ then $3(i - j) \equiv 0 \pmod{p}$, but $i - j \neq 0$ because $w(x, z) = 3$, and therefore $3 \equiv 0 \pmod{p}$, which means that $p = 3$.

The other direction is trivial. \square

THEOREM 2.22. For $p > 3$, if $x \xleftrightarrow[d]{2} z$ then $d \neq 3$.

PROOF. Assume to the contrary, that $l(z, x) = 3$. Then $x = x_i + x_j + x_k$ and $z = z_m + z_n$ for some $m, n, i, j, k \in \mathbb{Z}/p\mathbb{Z}$. Since $p > 3$, at least two of the following hold: $i + k \not\equiv 2j \pmod{p}$, $j + k \not\equiv 2i \pmod{p}$, $i + j \not\equiv 2k \pmod{p}$, because otherwise $p = 3$ according to Lemma 2.21. Without loss of generality we may assume that $i + k \not\equiv 2j \pmod{p}$ and $j + k \not\equiv 2i \pmod{p}$.

Let us look at the equation $[x, x, z]_{m,n} = 0$. If we take only the part which ρ^{2i} -commutes with z we get $(\rho^{-i} - \rho^m)(\rho^{-i} - \rho^n)x_i^2z = 0$, and if we take only the part which ρ^{2j} -commutes with z we get $(\rho^{-j} - \rho^m)(\rho^{-j} - \rho^n)x_j^2z = 0$. Consequently, $m = -i$ and $n = -j$ without loss of generality. If we take only the part which ρ^{i+k} -commutes with z we obtain $(\rho^{-k} - \rho^{-i})\rho^{-i}x_kx_iz - (\rho^{-k} - \rho^{-i})\rho^{-k}x_ix_kz = 0$. Consequently, $x_ix_k = \rho^{k-i}x_kx_i$. Similarly $x_jx_k = \rho^{k-j}x_kx_j$.

Now let us look at the equality $[z, z, x]_{i,j} = (\rho^k - \rho^i)(\rho^k - \rho^i)z^2x_k$. If we substitute $z = z_{-i} + z_{-j}$ on the left-hand side of this equation then we get $(\rho^j - \rho^i)\rho^iz_{-j}z_{-i} - (\rho^j - \rho^i)\rho^jz_{-j}z_{-i} = (\rho^k - \rho^i)(\rho^k - \rho^i)x_k$.

Consequently, $x_k \rho^{-i-j}$ -commutes with x . If $k = 0$ it means that x_k commutes with x and then $x_i = x_j = 0$. Otherwise, it means that the part of x which commutes with x_k is equal to zero, but this part is also equal to x_k , hence $x_k = 0$. At any rate, we have a contradiction. \square

PROPOSITION 2.23. For $p = 5$ if $x \xrightarrow{\{i,j\}} z$ and $z_i \xrightarrow{2} z_j$ then there exists a Rost chain of length 3 connecting x and z .

PROOF. Let $l(x, z) = \{i, j\}$ and $l(z_i, z_j) = \{m, n\}$. Without loss of generality we can assume that $m = 1$ and $n = 3$ or $n = 4$. According to Proposition 2.14, the case of $n = 4$ is not possible, and so we assume that $n = 3$.

The space $Fz_i + Fz_j$ is a short 5-central of type $\{1, 3\}$ and his exponentiation form is diagonal. In [CV12] it is proven that in this case either $z_{j,1}z_{j,3} = \rho z_{j,3}z_{j,1}$ or $z_{j,1}z_{j,3} = \rho^2 z_{j,3}z_{j,1}$.

In the case the Rost chain $z \longleftrightarrow z_{j,1}^{-1}(z_i + z_{j,3}) \longleftrightarrow z_{j,1} \longleftrightarrow x$. In the second case the Rost chain is $z \longleftrightarrow z_{j,3}^{-1}(z_i + z_{j,1}) \longleftrightarrow z_{j,3} \longleftrightarrow x$. \square

THEOREM 2.24. *For $p = 5$, if $x \xrightarrow{\{i,j\}} z$ then $w(z_i, z_j) \neq 3$.*

PROOF. If $l(z_i, z_j) = \{m, n, k\}$ then without loss of generality $m \equiv -n \pmod{5}$ and $m, n \not\equiv -k \pmod{5}$.

The space $Fz_i + Fz_j$ is a p -central with a diagonal exponentiation form according to Corollary 2.9. From the relation $(z_i)^3 * (z_j)^2 = 0$ we get $z_{j,m}z_{j,n} = \rho^m z_{j,n}z_{j,m}$. But again, as in the proof of Proposition 2.14, it means that $2j \equiv i^2 \pmod{p}$. As before, we shall have a contradiction, because we get $2(2j) \equiv (2i)^2 \pmod{p}$ as well. \square

REMARK 2.25. *There are however cases where $x \xrightarrow{\{i,j\}} z$ and $z_i \xrightarrow{2} z_j$ or $z_i \xrightarrow{4} z_j$. In particular, if $A = F[x, y : x^5 = \alpha, y^5 = \beta, yx = \rho xy]$ and $z = y + (a_1x + a_2x^2 + a_3x^3 + a_4x^4)y^{-1}$ then z is p -central if and only if $a_2a_3 = (\rho^4 - \rho)a_1a_4$. Consequently, if we take $a_3 = a_4 = 0$ then $w(x, z) = 2$ and $w(z_1, z_{-1}) = 2$, and if we take $a_1 = a_4 = a_3 = 1$ and $a_2 = (\rho^4 - \rho)$ then $w(x, z) = 2$ while $w(z_1, z_{-1}) = 4$. The case of $z_i \xrightarrow{5} z_j$ is not possible, due to Corollary 2.10.*

PROOF. In order to prove the statement “ $z = y + (a_1x + a_2x^2 + a_3x^3 + a_4x^4)y^{-1}$ then z is p -central if and only if $a_2a_3 = (\rho^4 - \rho)a_1a_4$ ” one should turn to the relations $z_1 * z_4^4 = z_1^2 * z_4^3 = z_1^3 * z_4^2 = z_1^4 * z_4 = 0$ ($z_1 = y$ and $z_4 = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4)y^{-1}$). On one hand, these relations are satisfied if and only if $z \in \mathcal{X}$ (Corollary 2.9). On the other hand, it can be checked that these relations are satisfied if and only if $a_0 = 0$ and $a_2a_3 = (\rho^4 - \rho)a_1a_4$:

Due to the relation $y_1^4 * y_4 = 0$ we have $a_0 = 0$. Write $w_i = a_i x^i y_1^{-1}$.

Now, the relation $y_1^3 * y_4^2 = 0$ provides the following due to conjugation by y_1 :

- (1) $y_1^3 * w_3^2 + y_1^3 * w_2 * w_4 = 0$
- (2) $y_1^3 * w_1^2 + y_1^3 * w_3 * w_4 = 0$
- (3) $y_1^3 * w_4^2 + y_1^3 * w_1 * w_2 = 0$
- (4) $y_1^3 * w_2^2 + y_1^3 * w_1 * w_3 = 0$
- (5) $y_1^3 * w_1 * w_4 + y_1^3 * w_2 * w_3 = 0$

The first four relations are trivial. From the fifth we obtain $5(\rho + 1 + \rho^{-1})a_1a_4\alpha y_1 + 5(\rho^3 + \rho^2 + 1)a_2a_3\alpha y_1 = 0$. Consequently, $a_2a_3 = (\rho^4 - \rho)a_1a_4$.

The relation $y_1^2 * y_4^3$ provides the following due to conjugation by y_1 :

- (1) $y_1^2 * w_1 * w_2^2 + y_1^2 * w_1^2 * w_3 + y_1^2 * w_2 * w_4^2 + y_1^2 * w_3^2 * w_4 = 0$
- (2) $y_1^2 * w_1 * w_2 * w_3 + y_1^2 * w_1^2 * w_4 + y_1^2 * w_2^3 + y_1^2 * w_3 * w_4^2 = 0$
- (3) $y_1^2 * w_1 * w_2 * w_4 + y_1^2 * w_2^2 * w_3 + y_1^2 * w_4^3 + y_1^2 * w_1 w_3^2 = 0$
- (4) $y_1^2 * w_1^3 + y_1^2 * w_1 * w_3 * w_4 + y_1^2 * w_2 * w_3^2 + y_1^2 * w_2^2 * w_4 = 0$
- (5) $y_1^2 * w_3^3 + y_1^2 * w_2 * w_3 * w_4 + y_1^2 * w_1 * w_4^2 + y_1^2 * w_1^2 * w_2 = 0$

The first relation is trivial. The second relation implies that $5(\rho^3 + \rho^2 + 1)a_1a_2a_3\alpha xy^{-1} + 5(\rho + 1 + \rho^{-1})a_1^2a_4\alpha xy_1^{-1} = 0$. This is automatically satisfied given $a_2a_3 = (\rho^4 - \rho)a_1a_4$. The same happens with the succeeding relations.

The relation $y_1 * y_4^4$ provides the following due to conjugation by y_1 :

- (1) $y_1 * w_1 * w_2 * w_3 * w_4 + y_1 * w_1^2 * w_4^2 + y_1 * w_2^2 * w_3^2 + y_1 * w_2^3 * w_4 + y_1 * w_3 * w_4^3 + y_1 * w_1 * w_3^3 + y_1 * w_1^3 * w_2 = 0$
- (2) $y_1 * w_1^3 * w_3 + y_1 * w_1^2 * w_2^2 + y_1 * w_1 * w_2 * w_4^2 + y_1 * w_1 * w_3^2 * w_4 + y_1 * w_2^2 * w_3 * w_4 + y_1 * w_2 * w_3^3 + y_1 * w_4^4 = 0$
- (3) $y_1 * w_2^3 * w_1 + y_1 * w_2^2 * w_4^2 + y_1 * w_2 * w_4 * w_3^2 + y_1 * w_2 * w_1^2 * w_3 + y_1 * w_4^2 * w_1 * w_3 + y_1 * w_4 * w_1^3 + y_1 * w_3^4 = 0$
- (4) $y_1 * w_3^3 * w_4 + y_1 * w_3^2 * w_1^2 + y_1 * w_3 * w_1 * w_2^2 + y_1 * w_3 * w_4^2 * w_2 + y_1 * w_1^2 * w_4 * w_2 + y_1 * w_1 * w_4^3 + y_1 * w_2^4 = 0$
- (5) $y_1 * w_4^3 * w_2 + y_1 * w_4^2 * w_3^2 + y_1 * w_4 * w_3 * w_1^2 + y_1 * w_4 * w_2^2 * w_1 + y_1 * w_3^2 * w_2 * w_1 + y_1 * w_3 * w_2^3 + y_1 * w_1^4 = 0$

All these relations are trivial. \square

THEOREM 2.26. *If $x \xrightarrow{2} z$, and $0 \notin l(z, x)$ then there is a Rost chain connecting x and z .*

PROOF. The case of $0 \in l(x, z)$ has already been dealt with (Corollary 2.13). The same goes for $w(z, x) = 2$ (Theorem 2.11).

Since $w(x, z) = 2$, $w(z, x) \neq 3$ (as in Theorem 2.22).

Let us assume that $0 \notin l(x, z)$ and $w(z, x) = 4$. Consequently, $l(x, z) \subseteq l(z, x)$.

There are two distinct cases: $l(x, z) = \{1, 4\}$ and $l(x, z) = \{1, 3\}$.

Assume $l(x, z) = \{1, 4\}$. By taking the part of equality $[x, x, z]_{4,1} = 0$ which ρ^3 -commutes with z we obtain $(zx_2 - \rho^4x_2z)x_1 - \rho x_1(zx_2 - \rho^4x_2z) = 0$. Consequently $(\rho^3 - \rho^4)\rho^4x_2x_1z - (\rho^3 - \rho^4)\rho x_1x_2z = 0$, which means that $x_1x_2 = \rho^3x_2x_1$. Therefore $x_2 = ax_1^2z^3$ for some $a \in F$.

Now, by taking the part of the equality $[x, x, z]_{4,1} = 0$ which ρ^4 -commutes with z we obtain $(zx_3 - \rho^4 x_3 z)x_1 - \rho x_1(zx_3 - \rho^4 x_3 z) + (zx_2 - \rho^4 x_2 z)x_2 - \rho x_2(zx_2 - \rho^4 x_2 z) = 0$. Hence $x_3 = \frac{(\rho^3 - \rho^4)(\rho^3 - \rho)}{(\rho^2 - \rho^4)(\rho^3 - \rho)} a \rho z^5 x_1^3 z + b x_1^3 z^3$ for some $b \in F$, i.e. $x_3 = (-\rho^3 - 1) a z^5 x_1^3 z + b x_1^3 z^3$.

By taking the part of the equality $[x, x, z]_{1,4} = 0$ which ρ^2 -commutes with z we obtain $(zx_3 - \rho x_3 z)x_4 - \rho^4 x_4(zx_3 - \rho x_3 z) = 0$. Consequently $(\rho^2 - \rho)\rho x_3 x_4 z - (\rho^2 - \rho)\rho^4 x_4 x_3 z = 0$, which means that $x_3 x_4 = \rho^3 x_4 x_3$. Therefore $x_4 = c x_3^3 z$ for some $c \in F$.

By taking the part of the equality $[x, x, z]_{1,4} = 0$ which ρ -commutes with z we obtain $(zx_2 - \rho x_2 z)x_4 - \rho^4 x_4(zx_2 - \rho x_2 z) + (zx_3 - \rho x_3 z)x_3 - \rho^4 x_3(zx_3 - \rho x_3 z) = 0$. Now, by taking the projection on the line $F x_1 z^4$, we get that $b = 0$.

Henceforth $x \in F[x_1 z^3]x_1$, which means that $x \longleftrightarrow x_1 z^3 \longleftrightarrow z$.

Assume $l(x, z) = \{1, 3\}$. Then we have the following equality $(\rho^4 - \rho)(\rho^4 - \rho^2)(\rho^4 - \rho^3)z^3 x_4 = [z, z, z, x]_{1,2,3}$. Substituting $z = z_1 + z_3$ in this equality we get that $l(x, x_4) = \{0, 2\}$. Consequently there is a Rost chain between x and x_4 , and because $w(x_4, z) = 1$, there is also a Rost chain between x and z . \square

3. The Chain Lemma for Biquaternion Algebras

For quaternion algebras, regardless of the characteristic, it is known that given two presentations of the same algebra, one could move from one presentation to the other by a chain of up to three steps, such that each step preserves one entry unchanged.

In characteristic not two, if two presentations of the same algebra share a common slot, $(\alpha, \beta) = (\alpha, \beta')$, then it is easy to see that $\beta' = (a^2 - b^2\alpha)\beta$ for some $a, b \in F$.

As a result, all of the different presentations of a given quaternion algebra (α, β) can be obtained by a series of steps such that in each step we choose $a, b \in F$ and change the symbol either to $(\alpha, (a^2 - b^2\alpha)\beta)$ or $((a^2 - b^2\beta)\alpha, \beta)$.

In characteristic two, if $[\alpha, \beta] = [\alpha, \beta']$ then it is easy to see that $\beta' = (a^2 + ab + b^2\alpha)\beta$ for some $a, b \in F$. If $[\alpha, \beta] = [\alpha', \beta]$ then $\alpha' = \alpha + a^2 + a + b^2\beta$ for some $a, b \in F$.

As a result, all of the different presentations of a given quaternion algebra $[\alpha, \beta]$ can be obtained by a series of steps such that in each step we choose $a, b \in F$ and change the symbol either to $[\alpha, (a^2 + ab + b^2\alpha)\beta]$ or $[\alpha + a^2 + a + b^2\beta, \beta]$.

The chain lemma for biquaternion algebras in characteristic not two, i.e. algebras of the form $(\alpha, \beta) \otimes (\gamma, \delta)$, was studied recently in [Siv12] and [CV13]. In the latter, the chain lemma was studied through quadruples of generators, i.e. a quadruple (x, y, z, u) such that $x^2 = \alpha, y^2 = \beta, z^2 = \gamma, u^2 = \delta, xy = -yx, xz = zx, xu = ux, yz = zy, yu = uy, zu = -uz$. The quadruple is divided into two pairs, (x, y) and (z, u) . The first one corresponds to the first symbol and the other to the second.

In [CV13] the following changes of quadruples of generators are defined:

- Λ_3 : At most three generators are changed.
- Λ_2 : At most one generator is changed in each pair.
- Π : At most one pair is changed.
- Ω : Two generators, one from each pair, are multiplied by the same element from the field generated over F by the product of the two remaining generators.
- Λ_1 : At most one generator is changed.

It was proven in that paper that every two non-commuting square-central elements have a third square-central element commuting with them both. It is rather easy to prove, using techniques that had been known already to Albert (see [Alb61]) that because of this fact, every two different symbol presentations of the same biquaternion algebra are connected by a chain of up to three steps of type Λ_3 (as opposed to five steps of type Λ_3 and ten of type Π as written in [CV13]). In that paper, it was also proven that each step of type Λ_3 can be achieved by five steps of type Λ_2 ; Each step of type Λ_2 can be achieved by one step of type Ω and two of type Λ_1 ; A step of type Π is known to be achieved by three steps of type Λ_1 . All in all, one can move from one symbol presentation of the algebra to another by at most 6 steps of type Ω and 39 of type Λ_1 (as opposed to 10 and 135 in [CV13]).

In this section we prove a similar chain lemma for biquaternion algebras in case of characteristic 2. We study it through quadruples of standard generators. A quadruple of generators is (x, y, z, u) such that

$$x^2 + x = \alpha, y^2 = \beta, z^2 + z = \gamma, u^2 = \delta,$$

$$xy + yx = y, xz = zx, xu = ux, yz = zy, yu = uy, zu + uz = u$$

where $[\alpha, \beta] \otimes [\gamma, \delta]$ is the algebra under discussion. The quadruple consists naturally of two pairs, (x, y) and (z, u) . We are not concerned with the order of the pairs, i.e. $(x, y, z, u) = (z, u, x, y)$. Of course the order of the elements inside the pair is important, the first element

corresponds to a separable field extension of the center and the second corresponds to an inseparable field extension. The first element is Artin-Schreier, and the second element is square-central.

We define the following steps on a quadruple of generators (x, y, z, u) :

- Λ_3 : At most three generators are changed.
- Λ_2 : At most one generator is changed in each pair.
- Π : At most one pair is changed.
- Ω_s : x and z are preserved and y and u are multiplied by $a + b(x + z)$ for some $a, b \in F$
- Ω_i : y and u are preserved and an element of the form ayu is added to x and z for some $a \in F$.
- Ω_c : y and z are preserved and x changes to $x + by(1 + by)^{-1}z$ and u changes to $(1 + by)u$ for some $b \in F$.
- Λ_1 : At most one generator is changed.

We prove that one can move from one quadruple of generators to another by a chain consisting of up to three steps of type Λ_3 . We prove further that every step of type Λ_3 can be replaced with up to three steps of type Π and two steps of type Λ_2 . Furthermore, we prove that each step of type Λ can be replaced with up to either three steps of type Λ_1 or two of type Λ_1 and one of type Ω_i , Ω_s or Ω_c . Since Π changes only one quaternion algebra, it is known that Π can be replaced with up to three steps of type Λ_1 . Consequently, in order to move from one quadruple of generators to another one needs to do up to 45 steps, where at most 6 of them are of type Ω_i , Ω_s or Ω_c and all the rest are of type Λ_1 .

The basic steps on the quadruples of generators can be easily translated to basic steps on the symbol presentations.

The Ω_s step changes $[\alpha, \beta) \otimes [\gamma, \delta)$ to

$$[\alpha, (a^2 + ab + b^2(\alpha + \gamma))\beta) \otimes [\gamma, (a^2 + ab + b^2(\alpha + \gamma))\delta)$$

for some given $a, b \in F$.

The Ω_i step changes $[\alpha, \beta) \otimes [\gamma, \delta)$ to

$$[\alpha + a^2\beta\delta, \beta) \otimes [\gamma + a^2\beta\delta, \delta)$$

for some given $a \in F$.

The Ω_c step changes $[\alpha, \beta) \otimes [\gamma, \delta)$ to $[\alpha + \frac{b^2\beta\gamma}{1+b^2\beta}, \beta) \otimes [\gamma, \delta(1 + b^2\beta))$ for some $b \in F$.

The Λ_1 step changes one of the quaternion algebras $[\alpha, \beta)$ to either to $[\alpha, (a^2 + ab + b^2\alpha)\beta)$ or $[\alpha + a^2 + a + b^2\beta, \beta)$ for some $\alpha, \beta \in F$.

Throughout this paper, let A be a fixed biquaternion division algebra over a field F of characteristic two.

3.1. Decomposition with respect to maximal subfields. In this section we shall prove that if A contains a maximal subfield, generated either by two Artin-Schreier elements or one Artin-Schreier and one square-central, then it decomposes as the tensor product of two quaternion algebras such that each of the generators is contained in a different quaternion algebra.

These lemmas will be used later on in this paper.

LEMMA 3.1. *If x and z are commuting Artin-Schreier elements then there exist some square-central elements u and y such that (x, y, z, u) is a quadruple of generators.*

PROOF. If x and z are commuting Artin-Schreier elements then $C_A(F[x])$ is a quaternion algebra containing z . This algebra contains some q such that $q^2 \in F[x]$ and $zq + qz = q$. The involution on $F[x, z]$ satisfying $x^* = x + 1$ and $z^* = z$ extends to A . In particular, $q^*x = xq^*$, and therefore $q^* \in C_A(F[x])$. If $q^* = q$ then by taking $u = q$, u is square-central and $zu + uz = u$. Otherwise, we take $u = q + q^*$. In particular $A = A_0 \otimes F[z, u]$. x is in the quaternion subalgebra A_0 and therefore there exists some square-central element $y \in A_0$ such that $xy + yx = y$. \square

LEMMA 3.2. *If x is Artin-Schreier, u is square-central and $xu = ux$, then there exist some Artin-Schreier element z and some square-central element y such that (x, y, z, u) is a quadruple of generators.*

PROOF. If x is Artin-Schreier and u is a square-central element commuting with x then $C_A(F[x])$ is a quaternion algebra containing u . This algebra contains some q such that $q^2 + q \in F[x]$ and $qu + uq = u$. The involution on $F[x, u]$ satisfying $x^* = x + 1$ and $u^* = u$ extends to A . In particular, $q^*x = xq^*$, and therefore $q^* \in C_A(F[x])$.

For some $\beta \in F$, $u^2 = \beta$. Write $\mu = q(a + bu)q^*$ for some unknown $a, b \in F$. Since $q + q^*$ is symmetric with respect to $*$ and commutes with u , $q + q^* = c + du$ for some fixed $c, d \in F$. Obviously $\mu^* = \mu$. We want $\mu u + u\mu = u$. It is a straight-forward calculation to see the condition becomes $1 = a + ac + bd\beta + (ad + bc)u$. Consequently, we want the following system to be satisfied:

$$\begin{aligned} 1 &= (c + 1)a + d\beta b \\ 0 &= da + cb \end{aligned}$$

This system has a solution, unless $c(c+1) = d^2\beta$.

If $c(c+1) \neq d^2\beta$ then by taking $z = q(a+bu)q^*$ where a, b is a solution to the system above, z is Artin-Schreier and $zu + uz = u$.

If $c(c+1) = d^2\beta$ then $(q^*)^2 + q^* = (q+c+du)^2 + (q+c+du) = q^2 + c^2 + d^2\beta + du + q + c + du = q^2 + q$. This means that $q^2 + q$ is invariant under $*$, and therefore $q^2 + q \in F$. In this case we will take $z = q$.

All in all, one can find an Artin-Schreier element z such that $zu + uz = u$ and $xz = zx$, which means that $A = A_0 \otimes F[z, u]$. x is in the quaternion subalgebra A_0 and therefore there exists some square-central element $y \in A_0$ such that $xy + yx = y$. \square

3.2. A chain consisting of steps of type Λ_3 . In this section we will show that every two generating quadruples are connected by a chain of up to three steps of type Λ_3 .

LEMMA 3.3. *For any two Artin-Schreier elements x, z , if they do not commute then the subalgebra $F[x, z]$ is a quaternion algebra, whose center is either F or a quadratic extension of it.*

PROOF. There exist $a, b \in F$ such that $x^2 + x = a$ and $z^2 + z = b$. Let $r = xz + zx$, $t = xz + zx + z = r + z$. It is easy to see that $xr + rx = r$, and $xt + tx = 0$.

Since $z = r + t$, $z^2 + z + b = r^2 + t^2 + rt + tr + r + t + b = 0$. Therefore $(z^2 + z + b)x + x(z^2 + z + b) = rt + tr + r = 0$.

Since $s = x + t$ commutes with x, t, r , it is in the center of $F[x, z]$. The elements x and r generate a quaternion algebra over the center of $F[x, z]$, and since t differs from x by a central element, $F[x, z]$ is a quaternion algebra over its center.

Since $F[x, z]$ is a subalgebra of a biquaternion algebra, it cannot be the entire algebra, and therefore its center is either F or a quadratic field extension of F . \square

LEMMA 3.4. *If x and z are not commuting Artin-Schreier elements then there exists some $w \in V$ which is either Artin-Schreier or square-central and commutes with them both.*

PROOF. If the center of $F[x, z]$ is a quadratic extension of F then it is generated by some $w \in V$, and that finishes the proof. Otherwise, according to Lemma 3.3 the center of $F[x, z]$ is F and $A = F[x, z] \otimes F[w, u : w^2 + w = c, u^2 = d, wu + uw = u]$ for some $c, d \in F$, and this also finishes the proof. \square

THEOREM 3.5. *Every two quadruples of generators are connected by a chain of up to three steps of type Λ_3 .*

PROOF. Let (x, y, z, u) and (x', y', z', u') be two quadruples of generators. If x and x' are not commuting then according to Lemma 3.4 there exists some w which is either Artin-Schreier or square-central commuting with x and x' .

If w is Artin-Schreier then according to Lemma 3.1 there exist $s, t \neq 0$ such that (x, s, w, t) is a quadruple of generators.

Similarly, there exist some s', t' such that (x', s', w, t') is a quadruple of generators.

Consequently, there is a chain

$$(x, y, z, u) \xrightarrow{\Lambda_3} (x, s, w, t) \xrightarrow{\Lambda_3} (x', s', w, t') \xrightarrow{\Lambda_3} (x', y', z', u').$$

If w is square-central then according to Lemma 3.2 there exist $s, t \neq 0$ such that (x, s, t, w) is a quadruple of generators.

Similarly, there exist some s', t' such that (x', s', t', w) is a quadruple of generators.

Consequently, there is a chain

$$(x, y, z, u) \xrightarrow{\Lambda_3} (x, s, t, w) \xrightarrow{\Lambda_3} (x', s', t', w) \xrightarrow{\Lambda_3} (x', y', z', u').$$

If x and x' are commuting then according to Lemma 3.1 there exist $s, t \neq 0$ such that (x, s, x', t) is a quadruple of generators.

Consequently, there is a chain

$$(x, y, z, u) \xrightarrow{\Lambda_3} (x, s, x', t) \xrightarrow{\Lambda_3} (x', y', z', u').$$

□

3.3. Replacing a step of type Λ_3 with steps of types Π and Λ_2 . In this section we shall show how a step of type Λ_3 can be obtained by up to three steps of type Π and two of type Λ_2 .

LEMMA 3.6. *If y and y' are two non-commuting square-central elements in A then $F[y, y']$ is a quaternion algebra either over F or over a quadratic extension of F . In particular, there exists either an Artin-Schreier element or a square-central element that commutes with both of them.*

PROOF. Let $t = yy' + y'y$ and $r = yy' + y'y + y'$. It is easy to see that $yt = ty$, $y't = ty'$ and $yr + ry = t$. In particular t is in the center of $F[y, y']$. If $t = 0$ then $y' = r$ and y' commutes with y , but we assumed the contrary, and so $t \neq 0$. For similar reasons $r \neq 0$.

Let $q = yrt^{-1}$. It is a straight-forward calculation to see that $q \in V$ and $qr + rq = r$. Consequently q and r generate a quaternion algebra over the center of $F[y, y']$. Since this center contains t , it is easy to see that y and y' belong to that quaternion algebra, and therefore $F[y, y'] = K[q, r]$ where $K = Z(F[y, y'])$. Since it is a subalgebra of a biquaternion algebra over F , its center can be either F or a quadratic extension of F . In both cases there exists either an Artin-Schreier element or a square-central element that commutes with both y and y' . \square

THEOREM 3.7. *Every step of type Λ_3 can be achieved by at most three steps of type Π and two of type Λ_2 .*

PROOF. A step of type Λ_3 preserves either an Artin-Schreier generator or a square-central generator.

Assume that it preserves an Artin-Schreier generator, i.e.

$$(x, y, z, u) \xrightarrow{\Lambda_3} (x, y', z', w').$$

If $y' \in F[x, y]$ then

$$(x, y, z, u) \xrightarrow{\Lambda_1} (x, y', z, u) \xrightarrow{\Pi} (x, y', z', u').$$

Otherwise, if y' commutes with y then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, ?, yy') \xrightarrow{\Lambda_2} (x, y', ?, yy') \xrightarrow{\Pi} (x, y', z', u').$$

Assume that they do not commute. According to Lemma 3.6, there exists either an Artin-Schreier element or a square-central element t commuting with both y and y' .

If $\mu = xt + tx + t \notin F$ then it is a straight-forward calculation to show that μ commutes with x, y and y' , and so μ generates a quadratic extension in both $F[z, u]$ and $F[z', u']$. If it is separable then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, \mu, ?) \xrightarrow{\Lambda_2} (x, y', \mu, ?) \xrightarrow{\Pi} (x, y', z', u'),$$

and if inseparable then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, ?, \mu) \xrightarrow{\Lambda_2} (x, y', ?, \mu) \xrightarrow{\Pi} (x, y', z', u').$$

Otherwise, t could be picked such that $\mu = 0$ and then $xt + tx = t$, and therefore t must be square-central. In this case

$$\begin{aligned} (x, y, z, u) &\xrightarrow{\Pi} (x, y, ?, ty) \xrightarrow{\Lambda_2} (x, t, ?, ty) \\ &\xrightarrow{\Pi} (x, t, ?, ty') \xrightarrow{\Lambda_2} (x, y', ?, ty') \xrightarrow{\Pi} (x, y', z', u'). \end{aligned}$$

Assume that the initial Λ_3 -step preserves a square-central generator, i.e.

$$(x, y, z, u) \xrightarrow{\Lambda_3} (x', y, z', w').$$

If $x' \in F[x, y]$ then

$$(x, y, z, u) \xrightarrow{\Lambda_1} (x', y, z, w) \xrightarrow{\Pi} (x', y, z', w').$$

Otherwise, if x' commutes with x then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, x + x', ?) \xrightarrow{\Lambda_2} (x', y, x + x', ?) \xrightarrow{\Pi} (x', y, z', u').$$

Assume that they do not commute. According to Lemma 3.3, there exists either an Artin-Schreier element or a square-central element t commuting with both x and x' .

Let $\mu = t + yty^{-1}$. This element commutes with x , x' and y' . If $\mu \notin F$ then μ generates a quadratic extension in both $F[z, u]$ and $F[z', u']$. If it is separable then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, \mu, ?) \xrightarrow{\Lambda_2} (x, y', \mu, ?) \xrightarrow{\Pi} (x, y', z', u'),$$

and if inseparable then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, ?, \mu) \xrightarrow{\Lambda_2} (x, y', ?, \mu) \xrightarrow{\Pi} (x, y', z', u').$$

If $\mu = 0$ then t commutes with y and hence $t \in F[z, u]$. If t is square-central then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, t, ?) \xrightarrow{\Lambda_2} (x', y, t, ?) \xrightarrow{\Pi} (x', y, z', u'),$$

and if Artin-Schreier then

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, ?, t) \xrightarrow{\Lambda_2} (x', y, ?, t) \xrightarrow{\Pi} (x', y, z', u').$$

If $\mu \in F^\times$ then $(\mu^{-1}t)y + y(\mu^{-1}t) = y$, which means that $\mu^{-1}t$ is Artin-Schreier, but t was either Artin-Schreier or square-central to begin with, and therefore $\mu = 1$. In this case, $t + x, t + x' \notin F$, because otherwise x and x' commute, and we assumed that they do not. Now, $t + x$ commutes with both x and y , which means that it generates a quadratic extension of F inside $F[z, u]$, which means that either $a(t + x)$ is Artin-Schreier for some $a \in F^\times$ or $t + x$ is square-central. Similarly, $t + x'$ commutes with both x' and y , which means that it generates a quadratic extension of F inside $F[z', u']$, which means that either $a'(t + x')$ is Artin-Schreier for some $a' \in F^\times$ or $t + x'$ is square-central.

If $a(t + x)$ and $a'(t + x')$ are Artin-Schreier then we have

$$(x, y, z, u) \xrightarrow{\Pi} (x, y, a(t + x), ?) \xrightarrow{\Lambda_2} (t, y, a(t + x), ?)$$

$$\begin{aligned} & \xrightarrow{\Pi} (t, y, a'(t+x'), ?) \xrightarrow{\Lambda_2} (x', y, a'(t+x'), ?) \\ & \xrightarrow{\Pi} (x', y, z', u'). \end{aligned}$$

If $t+x$ and $t+x'$ are square-central then we have

$$\begin{aligned} (x, y, z, u) & \xrightarrow{\Pi} (x, y, ?, t+x) \xrightarrow{\Lambda_2} (t, y, ?, t+x) \\ & \xrightarrow{\Pi} (t, y, ?, t+x') \xrightarrow{\Lambda_2} (x', y, ?, t+x') \xrightarrow{\Pi} (x', y, z', u'). \end{aligned}$$

If $a(t+x)$ is Artin-Schreier and $t+x'$ is square central then we have

$$\begin{aligned} (x, y, z, u) & \xrightarrow{\Pi} (x, y, a(t+x), ?) \xrightarrow{\Lambda_2} (t, y, a(t+x), ?) \\ & \xrightarrow{\Pi} (t, y, ?, t+x') \xrightarrow{\Lambda_2} (x', y, ?, t+x') \xrightarrow{\Pi} (x', y, z', u'). \end{aligned}$$

The case of square-central $t+x$ and Artin-Schreier $a'(t+x')$ is essentially the same as the last one. \square

REMARK 3.8. *As a result, every two quadruples of generators are connected by a chain of up to 9 steps of type Π and 6 steps of type Λ_2 .*

3.4. Replacing a step of type Λ_2 with steps of types Ω_i , Ω_s , Ω_c and Λ_1 . In this section we shall show how a step of type Λ_2 can be obtained by up to three steps, one of which can be of type Ω_i , Ω_s or Ω_c and the others are of type Λ_1 . Since Π can be obtained by up to three steps of type Λ_1 , it means that every two quadruples of generators are connected by a chain of up to 45 steps, where up to 6 of them are of type Ω_i , Ω_s or Ω_c and the rest are of type Λ_1 .

LEMMA 3.9. *If a step of type Λ_2 preserves two inseparable generators, i.e. $(x, y, z, u) \xrightarrow{\Lambda_2} (x', y, z', u)$ then it can be achieved by at most two steps of type Λ_1 and one of type Ω_i .*

PROOF. The element $xz' + z'x + z'$ is nonzero because $(xz' + z'x + z')u + u(xz' + z'x + z') = u$. Consequently, $(x, y, xz' + z'x + z', u)$ is a quadruple of generators. Similarly, $(xz' + z'x + x, y, z', u)$ is a quadruple of generators. One can therefore do the following steps:

$$\begin{aligned} (x, y, z, u) & \xrightarrow{\Lambda_1} (x, y, xz' + z'x + z', u) \xrightarrow{\Omega_i} (xz' + z'x + x, y, z', u) \\ & \xrightarrow{\Lambda_1} (x', y, z', u). \end{aligned}$$

The element $r = xz' + z'x$ was added in the middle step to the Artin-Schreier generators. This element commutes with y and u , and therefore it is in $F[u, y]$ and consequently of the form $a + by + cu + dyu$. This element however also satisfies $xr + rx = z'r + rz' = r$. Hence, $a = b = c = 0$. \square

LEMMA 3.10. *If a step of type Λ_2 preserves two Artin-Schreier generators, i.e. $(x, y, z, u) \xrightarrow{\Lambda_2} (x, y', z, u')$ then it can be achieved by at most two steps of type Λ_1 and one of type Ω_s .*

PROOF. If $yu' + u'y = 0$ then y commutes with u' and then one can do

$$(x, y, z, u) \xrightarrow{\Lambda_1} (x, y, z, u') \xrightarrow{\Lambda_1} (x, y', z, u').$$

Otherwise, $yu' + u'y$ is square-central, and $(x, y, z, (yu' + u'y)y)$ is a quadruple of generators. Similarly $(x, (yu' + u'y)^{-1}u', z, u')$ is a quadruple of generators. One can therefore do

$$(x, y, z, u) \xrightarrow{\Lambda_1} (u, y, z, (yu' + u'y)y) \xrightarrow{\Omega_s} (x, (yu' + u'y)^{-1}u', z, u') \xrightarrow{\Lambda_1} (x, y', z, u').$$

In the middle step, the square-central generators were multiplied by $q = y^{-1}(yu' + u'y)^{-1}u'$. This element commutes with x and z and therefore $q \in F[x, z]$ and consequently of the form $a + bx + cz + dxz$. However, q commutes with yu' , and therefore $d = 0$ and $b = c$. \square

LEMMA 3.11. *If a step of type Λ_2 preserves one Artin-Schreier generator and one square-central generator, i.e. $(x, y, z, u) \xrightarrow{\Lambda_2} (x', y, z, u')$ then it can be achieved by either at most three steps of type Λ_1 or at most two steps of type Λ_1 and one of type Ω_c .*

PROOF. If $xu' + u'x + u'$ is zero then $xu' + u'x = u'$. Therefore one can do $(x, y, z, u) \xrightarrow{\Lambda_1} (x, y, z, yu') \xrightarrow{\Lambda_1} (x', y, z, yu') \xrightarrow{\Lambda_1} (x', y, z, u')$.

Let us assume $xu' + u'x + u' \neq 0$.

$$\begin{aligned} x(xu' + u'x + u') + (xu' + u'x + u')x &= \\ x^2u' + xu'x + xu' + xu'x + u'x^2 + u'x &= \\ (x + \alpha)u' + xu' + u'(x + \alpha) + u'x &= \\ xu' + \alpha u' + xu' + u'x + \alpha u' + u'x &= 0. \end{aligned}$$

Therefore x commutes with $xu' + u'x + u'$. In fact, $(x, y, z, xu' + u'x + u')$ is a quadruple of generators, and in particular $xu' + u'x + u'$ is square-central. Now $x(xu' + u'x + u')^{-1}(xu' + u'x) + (xu' + u'x + u')^{-1}(xu' + u'x)x = (xu' + u'x + u')^{-1}(xu' + u'x)$, and $(xu' + u'x + u')^{-1}(xu' + u'x)$ commutes with z and $xu' + u'x + u'$, and therefore $(xu' + u'x + u')^{-1}(xu' + u'x) = by + cxy$ for some $b, c \in F$, but $(xu' + u'x + u')^{-1}(xu' + u'x)$ also commutes with $xu' + u'x$ while $y(xu' + u'x) + (xu' + u'x)y = 0$ and $xy(xu' + u'x) + (xu' + u'x)xy = y(xu' + u'x)$ and therefore $c = 0$. In particular $xu' + u'x = b(xu' + u'x + u')y$.

It is a straight-forward calculation to check that

$$(x + by(xu' + u'x + u')u'^{-1}z)u' + u'(x + by(xu' + u'x + u')u'^{-1}z) = 0,$$

$$(x + by(xu' + u'x + u')u'^{-1}z)z + z(x + by(xu' + u'x + u')u'^{-1}z) = 0,$$

and so $(x + by(xu' + u'x + u')u'^{-1}z, y, z, u')$ is a quadruple of generators too.

Therefore we have the chain

$$\begin{aligned} (x, y, z, u) &\xrightarrow{\Lambda_1} (x, y, z, xu' + u'x + u') \xrightarrow{\Omega_c} \\ (x + by(xu' + u'x + u')u'^{-1}z, y, z, u') &\xrightarrow{\Lambda_1} (x', y, z, u'). \end{aligned}$$

□

THEOREM 3.12. *Every two quadruples of elements are connected by a chain of up to 45 steps, of which up to 6 are of type Ω_i , Ω_s or Ω_c and the rest are of type Λ_1 .*

CHAPTER 4

Computational Aspects

1. Quadratic Elements and Quaternion Standard Equations

Let $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ be the real quaternion algebra, with $i^2 = j^2 = -1$, $k = ij$ and $ji = -k$.

Every element z in this algebra is therefore of the form $z = c_1 + c_2i + c_3j + c_4k$ where $c_1, c_2, c_3, c_4 \in \mathbb{R}$. Let $\Re(z) = c_1$ and $\Im(z) = z - \Re(z) = c_2i + c_3j + c_4k$. We call $\Re(z)$ the real part of z and $\Im(z)$ the imaginary part. If $\Re(z) = z$ then z is called pure real and if $\Im(z) = z$ then z is called pure imaginary. Every element z then can be written as the sum of two elements $r + x$ such that $r = c_1$ is pure real and $x = c_2i + c_3j + c_4k$ is pure imaginary. By easy calculation one can show that $x^2 = -(c_2^2 + c_3^2 + c_4^2) \in \mathbb{R}$.

The conjugate of z is defined to be $\bar{z} = r - x = c_1 - c_2i - c_3j - c_4k$. The norm of z is defined to be $N(z) = z\bar{z} = r^2 - x^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2 \in \mathbb{R}$. The norm is known to be a multiplicative function, i.e. $f(z_1z_2) = f(z_1)f(z_2)$, and for any $c \in \mathbb{R}$, $f(cz) = c^2f(z)$.

A quaternion polynomial equation with one indeterminate z is called standard if it is of the form $a_nz^n + \dots + a_1z + a_0 = 0$ for some $a_0, \dots, a_n \in \mathbb{H}$. Notice that since the quaternion algebra is noncommutative, the order of multiplication is crucial, for instance the equations $az^2 - b = 0$, $zaz - b = 0$ and $z^2a - b = 0$ are three distinct equations.

In [JO10b] Janovská and Opfer reduced the problem of solving any standard quaternion equation of degree n to a real equation of degree $2n$. However, for the case of $n = 2$ it is not optimal, since there are reductions into equations of degree 3 instead of 4 (see [HS02], [AY03]).

Here we present a new method for solving quaternion standard equations. For the case of $n = 2$ it is very similar to the techniques appearing in [HS02] and [AY03]. For the case of $n = 3$, if the equation has at least one pure imaginary root, then the problem is reduced to solving real equations of degrees no greater than 4, as opposed to the degree 6 equation that arises from the method in [JO10b].

Later in this section we shall use Wedderburn's decomposition method for standard quaternion polynomials. The ring of standard (or left) quaternion polynomials $\mathbb{H}[z]$ is simply the ring obtained by adding the variable z to the quaternion algebra with the relations $za = az$ for any $a \in \mathbb{H}$. The elements az^2 , zaz and z^2a are the same inside this ring. However, every polynomial $f(z)$ in that ring has a standard form, where the coefficients lie on the left-hand side of the variable, i.e. $f(z) = a_n z^n + \cdots + a_1 z + a_0$ for some $a_0, \dots, a_n \in \mathbb{H}$. When substituting an element $z_0 \in \mathbb{H}$ in $f(z)$ we substitute in the standard form, i.e. $f(z_0) = a_n z_0^n + \cdots + a_1 z_0 + a_0$. We call a a root of $f(z)$ if $f(a) = 0$. Consequently, finding the roots of a polynomial in this ring is equivalent to solving a standard quaternion equation.

It is important to mention that the substitution map $S_{z_0} : \mathbb{H}[z] \rightarrow \mathbb{H}$, taking $S_{z_0}(f(z)) = f(z_0)$, is not a ring homomorphism if z_0 is not pure real. For example, if $z_0 = i$, $g(z) = z - j$, $h(z) = z + j$ and $f(z) = g(z)h(z) = z^2 + 1$ then $g(i)h(i) = (i - j)(i + j) = 2k \neq 0$ while $f(i) = 0$.

The following statement is known to be true (see [Row92]): For given $f(z), g(z), h(z) \in \mathbb{H}[z]$, if $f(z) = g(z)h(z)$ and a is a root of $f(z)$ but not of $h(z)$ then $h(a)ah(a)^{-1}$ is a root of $g(z)$. Consequently, if $n = \deg(f)$ distinct roots of $f(z)$ are known then we can factorize $f(z)$ completely to linear factors. The opposite is not true, i.e. there is no simple algorithm for finding the roots of a polynomial knowing its factorization.

1.1. Roots of a quaternion standard polynomial. Let there be a monic polynomial $f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 \in \mathbb{H}[z]$ where $a_{k-1}, \dots, a_0 \in \mathbb{H}$ and $a_0 \neq 0$.

Similarly to the ring of standard polynomials with one variable $\mathbb{H}[z]$, one can look at the ring of polynomials with two variables $\mathbb{H}[r, N]$ where $ra = ar$ and $Na = aN$ for any $a \in \mathbb{H}$.

LEMMA 1.1. *There exist polynomials $g, h \in \mathbb{H}[r, N]$ such that $f(z_0) = g(r_0, N_0)x_0 + h(r_0, N_0)$ for any $z_0 \in \mathbb{H}$, $r_0 = \Re(z)$, $x_0 = \Im(z)$, $N_0 = -x_0^2$.*

PROOF. Let z_0 be some arbitrary element in \mathbb{H} . $f(z_0) = z_0^n + a_{n-1}z_0^{n-1} + \cdots + a_1z_0 + a_0$. Now, $z_0 = r_0 + x_0$ for some pure real r_0 and some pure imaginary x_0 . Since r_0 is real, it commutes with x_0 . Therefore $z_0^k = \sum_{m=0}^k \binom{k}{m} r_0^{m-k} x_0^m$. Let $N_0 = -x_0^2$. This element is pure real. For all $1 \leq k \leq n$, $z_0^k = (\sum_{m=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{2m+1} (-1)^m N_0^m r_0^{k-(2m+1)})x_0 + \sum_{m=0}^t \binom{k}{2m} (-1)^m N_0^m r_0^{k-2m}$.

Let $g_k(r, N) = \sum_{m=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{2m+1} (-1)^m N_0^m r_0^{k-(2m+1)}$ and $h(r, N) = \sum_{m=0}^t \binom{k}{2m+1} (-1)^m N_0^m r_0^{k-2m}$. Now let $g(r, N) = g_n(r, N) + a_{n-1}g_{n-1}(r, N) + \dots + a_1g_1(r, N)$ and $h(r, N) = h_n(r, N) + a_{n-1}h_{n-1}(r, N) + \dots + a_1h_1(r, N) + a_0$. It is easy to see that $f(z_0) = g(r_0, N_0)x_0 + h(r_0, N_0)$. \square

THEOREM 1.2. *Given an element $z_0 \in \mathbb{H}$, x_0, r_0, N_0 are as in Lemma 1.1, z_0 is a root of $f(z)$ if and only if one of the following conditions is satisfied:*

- (1) (r_0, N_0) is a solution to both $h(r, N) = 0$ and $g(r, N) = 0$.
- (2) (r_0, N_0) is a solution to the equation $-g(r, N)\overline{g(r, N)g(r, N)N} = h(r, N)\overline{g(r, N)h(r, N)}$ and $x_0 = -g(r_0, N_0)^{-1}h(r_0, N_0)$.

PROOF. If $h(r_0, N_0) = g(r_0, N_0) = 0$ then $f(z_0) = g(r_0, N_0)x_0 + h(r_0, N_0) = 0x_0 + 0 = 0$, i.e. z_0 is a root of $f(z)$.

If $h(r_0, N_0) \neq 0$ or $g(r_0, N_0) \neq 0$ while $f(z_0) = 0$, then $h(r_0, N_0) \neq 0$ and $\overline{g(r_0, N_0)} \neq 0$, because $\overline{g(r_0, N_0)x_0} = -h(N_0)$. Therefore $\overline{g(r_0, N_0)g(r_0, N_0)x_0} = N(g(r_0, N_0))x_0 = -\overline{g(r_0, N_0)h(r_0, N_0)}$.

Consequently
$$\overline{-N(g(r_0, N_0))^2 N_0} = \overline{g(r_0, N_0)h(r_0, N_0)g(r_0, N_0)h(r_0, N_0)},$$
 i.e. $-g(r_0, N_0)N(g(r_0, N_0))N_0 = \overline{g(r_0, N_0)h(r_0, N_0)g(r_0, N_0)h(r_0, N_0)}$. This is surely not the trivial equation, because the difference between the lowest degree among the nonzero monomials of the right-hand side of the equation and the lowest degree among the nonzero monomials of the left-hand side of the equation is at least 1. Consequently, (r_0, N_0) is a root of the equation $g(r, N)\overline{g(r, N)g(r, N)N} = h(r, N)\overline{g(r, N)h(r, N)}$. \square

1.2. Solving quadratic equations. Let $f(z) = z^2 + az + b$. By replacing z with $z - \frac{\Re(a)}{2}$, we may assume that $\Re(a) = 0$. The case of $a = 0$ is simple: If b is not pure real then the roots are $\pm \sqrt[4]{Nb}e^{\frac{\theta}{2} \frac{\Im(b)}{\sqrt{N(b)}}}$ where θ is the phase of b in its polar decomposition as a quaternion. If b is pure real then if it is negative then the roots are all the pure imaginary elements whose norms are real square roots of $N(b)$. Otherwise, the roots are the real positive and negative square roots of b .

Therefore we assume $a \neq 0$. We assumed that $\Re(a) = 0$ and therefore a is a nonzero pure imaginary. Taking $d = \frac{b+aba^{-1}}{2}$, it is clear that $ad = -da$ and $a(b-d) = (b-d)a$. Since $b-d$ commutes with a , it is of the form $m + na$ for some $m, n \in \mathbb{R}$. The case of $d = 0$ is again simple,

because then b commutes with a and the equation can be solved over the field $\mathbb{R}[a]$. Consequently we shall assume that $d \neq 0$.

Under this assumption, every equation of the form $z^2 + az + b = 0$ with $a, b \in \mathbb{H}$ can be brought to the form $z^2 + az + m + na + d = 0$ with $\Re(a) = 0$, $ad = -da$ and $m, n \in \mathbb{R}$.

THEOREM 1.3. *Assume $a, d \neq 0$. Let z_0 be a root of $f(z) = z^2 + az + m + na + d$. If $n \neq 0$ then $r_0 = \Re(z_0)$ is a solution to the equation $16r^6 + (-8a^2 + 16m)r^4 + (-a^2(4m - a^2) + 4a^2n^2 + 4d^2)r^2 - a^4n^2 = 0$ and $\Im(z_0) = -(2r_0 + a)^{-1}(\frac{1}{2r_0}a(r_0 + n)(2r_0 + a) + d)$. If $n = 0$ then one of the following happens:*

- (1) $r_0 = 0$, $N_0 = -\Im(z_0)^2$ is a solution to the equation $0 = N^2 + (a^2 - 2m)N + m^2 - d^2$ and $\Im(z_0) = -a^{-1}(m + d - N_0)$
- (2) r_0 is a solution to the equation $0 = 16r^4 + (-8a^2 + 16m)r^2 - a^2(4m - a^2) + 4d^2$ and $\Im(z_0) = -(2r_0 + a)^{-1}(\frac{1}{2}a(2r_0 + a) + d)$.

PROOF. The polynomials obtained according to the proof of Lemma 1.1 are in this case $g(r, N) = 2r + a$ and $h(r, N) = r^2 - N + ar + b$. Again $r_0 = \Re(z_0)$, $x_0 = \Im(z_0)$ and $N_0 = -x_0^2$.

Obviously $g(r_0, N_0) \neq 0$, therefore for according to Theorem 1.2, (r_0, N_0) is a solution to $-g(r, N)\overline{g(r, N)}g(r, N)N = h(r, N)\overline{g(r, N)}h(r, N)$.

We shall solve this equation then. $-(2r + a)(2r - a)(2r + a)N = (r^2 - N + ar + b)(2r - a)(r^2 - N + ar + b)$.

Taking only the part of the equation which anti-commutes with a we obtain

$$0 = d(2r - a)(r^2 - N + ar + m + na) + (2r - a)(r^2 - N + ar + m + na)d = ((2r + a)(r^2 - N - ar + m - na) + (2r - a)(r^2 - N + ar + m + na))d$$

Which means that $0 = (2r + a)(r^2 - N - ar + m - na) + (2r - a)(r^2 - N + ar + m + na) = 4r^3 - 4rN + 4rm - 2a^2r - 2na^2$.

If $n \neq 0$ then $r \neq 0$, and so $N = r^2 + m - \frac{1}{2}a^2 - \frac{1}{2r}na^2$.

$$h(r, N) = r^2 - N + ar + b = r^2 - (r^2 + m - \frac{1}{2}a^2 - \frac{1}{2r}na^2) + ar + m + na + d = \frac{1}{2}a^2 + \frac{1}{2r}na^2 + ar + na + d = \frac{1}{2r}a(r + n)(2r + a) + d$$

The equation of interest is $-(2r + a)(2r - a)(2r + a)N = h(r, N)(2r - a)h(r, N)$. Its part which commutes with a provides us with $-(2r + a)(2r - a)(2r + a)N = (\frac{1}{2r}a(r + n)(2r + a))(2r - a)(\frac{1}{2r}a(r + n)(2r + a)) + d(2r - a)d = \frac{1}{4r^2}(2r + a)(4r^2 - a^2)a^2(r + n)^2 + (2r + a)d^2$

Therefore $-(4r^2 - a^2)N = \frac{1}{4r^2}(4r^2 - a^2)a^2(r + n)^2 + d^2$, which means that $0 = \frac{1}{4r^2}(4r^2 - a^2)(4r^2(r^2 + m - \frac{1}{2}a^2 - \frac{1}{2r}na^2) + a^2(r + n)^2) + d^2 =$

$$\frac{1}{4r^2}(4r^2 - a^2)(4r^4 + 4r^2m - 2a^2r^2 - 2rna^2 + a^2r^2 + 2a^2rn + a^2n^2) + d^2 = \frac{1}{4r^2}(4r^2 - a^2)(4r^4 + 4r^2m - a^2r^2 + a^2n^2) + d^2.$$

Consequently $16r^6 + (-8a^2 + 16m)r^4 + (-a^2(4m - a^2) + 4a^2n^2 + 4d^2)r^2 - a^4n^2 = 0$.

If $n = 0$ then $0 = 4r^3 - 4rN + 4rm - 2a^2r = r(4r^2 - 4N + 4m - 2a^2)$, which means that either $r = 0$ or $N = r^2 + m - \frac{1}{2}a^2$. If $r = 0$ then $a^3N = (-N + m + d)(-a)(-N + m + d)$. Taking only the part which commutes with a we obtain $a^3N = -(-N + m)^2a + ad^2$, hence $a^2N = -N^2 + 2mN - m^2 + d^2$, and consequently $0 = N^2 + (a^2 - 2m)N + m^2 - d^2$.

If $N = r^2 + m - \frac{1}{2}a^2$ then $h(r, N) = r^2 - N + ar + b = r^2 - (r^2 + m - \frac{1}{2}a^2) + ar + m + d = \frac{1}{2}a^2 + ar + d = \frac{1}{2}a(2r + a) + d$. From $-(2r + a)(2r - a)(2r + a)N = h(r, N)(2r - a)h(r, N)$ we obtain $-(2r + a)(2r - a)(2r + a)N = (\frac{1}{2}a(2r + a) + d)(2r - a)(\frac{1}{2}a(2r + a) + d)$. Taking the part which commutes with a we get $-(2r + a)(2r - a)(2r + a)N = \frac{1}{4}a^2(2r + a)^2(2r - a) + (2r + a)d^2$. Therefore $-(4r^2 - a^2)N = \frac{1}{4}a^2(4r^2 - a^2) + d^2$, hence $0 = \frac{1}{4}(4r^2 - a^2)(4(r^2 + m - \frac{1}{2}a^2) + a^2) + d^2 = \frac{1}{4}(4r^2 - a^2)(4r^2 + 4m - a^2) + d^2$ and consequently $0 = 16r^4 + (-8a^2 + 16m)r^2 - a^2(4m - a^2) + 4d^2$. \square

1.3. Pure imaginary roots of a quaternion standard polynomial. Let $f(z)$, $g(r, N)$ and $h(r, N)$ as in Lemma 1.1. Let $g(N) = g(0, N)$ and $h(N) = h(0, N)$. For every pure imaginary z_0 , $f(z_0) = g(N_0)z_0 + h(N_0)$ where $N_0 = N(z_0) = -z_0^2$. In particular, $\deg(g) = \lfloor \frac{\deg f - 1}{2} \rfloor$ and $\deg h \leq \lfloor \frac{\deg f}{2} \rfloor$.

The following corollary is an easy result of Theorem 1.2:

COROLLARY 1.4. *A pure imaginary element z_0 of norm N_0 is a root of $f(z)$ if and only if one of the following conditions is satisfied:*

- (1) N_0 is a solution to both $h(N) = 0$ and $g(N) = 0$.
- (2) N_0 is a solution to the equation $-g(N)\overline{g(N)}g(N)N = h(N)\overline{g(N)}h(N)$ and $z_0 = -g(N_0)^{-1}h(N_0)$.

PROPOSITION 1.5. *The polynomial $f(z)$ has infinitely many pure imaginary roots if and only if $h(N) = 0$ and $g(N) = 0$ have a common real solution.*

PROOF. If $h(N) = 0$ and $g(N) = 0$ have a common real solution N_0 then every element $z_0 \in Q$ satisfying $-z_0^2 = N_0$ is a root of $f(z)$.

If $h(N)$ and $g(N)$ have no common root, and z_0 is a pure imaginary root of $f(z)$ of norm N_0 , then $h(N_0) \neq 0$ and $g(N_0) \neq 0$. On the other hand, N_0 is a solution to the equation $g(N)\overline{g(N)}g(N)N = h(N)\overline{g(N)}h(N)$. The degree of the left-hand side of this equation is

$3 \deg(g) + 1$, while the degree of the right-hand side is $2 \deg(h) + \deg(g)$. There is an equality only if $2 \deg(g) + 1 = 2 \deg(h)$, but that can never happen, therefore the equation is not trivial, which means that by splitting the equation into four (according to the structure of \mathbb{H} as a vector space over \mathbb{R} , i.e. $\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$) we have at least one nontrivial equation. Consequently, the number of roots of this system is finite, and therefore the number of pure imaginary roots of $f(z)$ is finite. \square

REMARK 1.6. *If z_0 is a pure imaginary root then $N(g(N_0))z_0 = -\overline{g(N_0)}h(N_0)$. Since $\Re(z_0) = 0$, we obtain $0 = \Re(-\overline{g(N_0)}h(N_0))$. If this equation is not trivial, then it has a finite set of roots which contains all the pure imaginary roots of the original equation.*

1.4. Solving cubic quaternion equations with at least one pure imaginary root.

LEMMA 1.7. *For any polynomial $p(z) \in \mathbb{H}[z]$, if $z_0 \neq a$ is a root of $f(z) = p(z)(z - a)$ then $0 = z_0^2 - (a + b)z_0 + ba$ for some root b of $p(z)$*

PROOF. According to Wedderburn's method, $b = (z_0 - a)z_0(z_0 - a)^{-1}$ is a root of $p(z)$. Hence $b(z_0 - a) = (z_0 - a)z$, i.e. $0 = z_0^2 - (a + b)z_0 + ba$. \square

REMARK 1.8. *If the decomposition into linear factors of a given polynomial $f(z) \in \mathbb{H}[z]$ is known, then the question of finding its roots becomes (inductively) a sequence of quadratic equations one has to solve. Over the quaternion algebra the quadratic equations are solvable and so one can obtain the roots of any standard polynomial if he knows its decomposition into linear factors.*

Let $f(z)$ be a quaternion standard cubic polynomial. The equation $-g(N)\overline{g(N)}g(N)N = h(N)\overline{g(N)}h(N)$ (from Corollary 1.4) is with one variable N and is of degree 4 at most, and therefore its real roots can be expressed in terms of radicals, which means that the pure imaginary roots of $f(z)$ can also be expressed in those terms.

Assume $f(z)$ has one such root a , then $f(z) = p(z)(z - a)$. The polynomial $p(z)$ is quadratic and therefore its roots can be formulated. Consequently, $p(z)$ can be fully factorized into linear factors and so is $f(z)$. Furthermore, according to Lemma 1.7, the roots of $f(z)$ are at hand.

1.4.1. Example. Consider the polynomial $f(z) = z^3 + (2 + ij)z + i - j \in \mathbb{H}[z]$.

$g(N) = -N + 2 + ij$ and $h(N) = i - j$. They have no common root, so we turn to solve $-g(N)N(g(N))N = h(N)\overline{g(N)}h(N)$ i.e. $-(-N + 2 + ij)((-N + 2)^2 + 1)N = (i - j)(-N + 2 - ij)(i - j)$, which means $-(-N + 2 + ij)(N^2 - 4N + 5)N = (-N + 2 + ij)(i - j)(i - j)$, and consequently

$$-(N^2 - 4N + 5)N = -2, \text{ and therefore}$$

$$N^3 - 4N^2 + 5N - 2 = 0.$$

In general this equation could be split into up to four equations according to the basis of \mathbb{H} as an \mathbb{R} -vector space. However, in this case, $N^3 - 4N^2 + 5N - 2$ is pure real and has no imaginary part, which means that we have to solve only one cubic real equation.

Therefore either $N = 1$ or $N = 2$. According to Theorem 1.2, the corresponding roots are $-g(N)^{-1}h(N)$, i.e. $z_1 = -\frac{1}{2}(1 - ij)(i - j) = -\frac{1}{2}(i - j - j - i) = j$ for $N = 2$ we have $z_2 = -(ij)^{-1}(i - j) = i + j$.

Consequently $f(z) = p(z)(z - j)$. Next goal is to calculate $p(z)$.

REMARK 1.9. *Let us recall how $f(z)$ is decomposed into $p(z)(z - a)$ given a root a :*

$$f(z) = z^n + c_{n-1}z^{n-1} + \dots + c_0$$

$$f(a) = a^n + c_{n-1}a^{n-1} + \dots + c_0$$

$$\begin{aligned} f(z) &= f(z) - 0 = f(z) - f(a) = (z^n - a^n) + c_{n-1}(z^{n-1} - a^{n-1}) + \dots + \\ c_1(z - a) &= ((z^{n-1} + az^{n-2} + \dots + a^{n-1}) + c_{n-1}(z^{n-2} + \dots + a^{n-2}) + \\ &\dots + c_1)(z - a) \end{aligned}$$

$$p(z) = (z^{n-1} + az^{n-2} + \dots + a^{n-1}) + c_{n-1}(z^{n-2} + \dots + a^{n-2}) + \dots + c_1.$$

Consequently $p(z) = (z^2 + jz - 1) + 2 + ij = z^2 + jz + 1 + ij$.

$-i - j$ is a root of $f(z)$ but not of $z - j$, hence according to Remark 1.9, $(-i - 2j)(-i - j)(-i - 2j)^{-1} = \frac{1}{5}(-i - 2j)(-i - j)(i + 2j) = \frac{1}{5}(-1 - 2ij + ij - 2)(i + 2j) = \frac{1}{5}(-3 - ij)(-i - j) = \frac{1}{5}(3i + 3j + j - i) = \frac{1}{5}(2i + 4j)$ is a root of $p(z)$.

The second and final root of $p(z)$ (which can be obtained using the methods) is i .

Again, due to Wedderburn, $p(z) = (z + i + 1 + ij)(z - i)$, which means that $f(z) = (z + 1 + i + ij)(z - i)(z - j)$

Let z_0 be some root of $f(z)$. According to Lemma 1.7, since i is a root of $p(z)$ and is different from $\frac{1}{5}(2i + 4j)$, z_0 must correspond to it, which means that $z_0^2 - (j + i)z_0 + ij = 0$. j is a root, however it is already known to be a root of $f(z)$ so we look for the other one. Let $t = z_0 - j$ and so $t^2 - it + tj = 0$. Let $r = t^{-1}$ and so $1 - ri + jr = 0$.

$r = c_1 + c_i i + c_j j + c_{ij} ij$, so we obtain the following linear system

$$(35) \quad 1 + c_i - c_j = 0$$

$$(36) \quad -c_1 + c_{ij} = 0$$

$$(37) \quad -c_{ij} + c_1 = 0$$

$$(38) \quad c_j - c_i = 0$$

This system has no solution. Therefore, $f(z)$ has no roots besides j and $i + j$.

1.5. A note on quadratic two-sided polynomials. A two-sided polynomial is a polynomial of the form $f(z) = z^n + a_{n-1}z^{n-1}b_{n-1} + \dots + a_1zb_1 + c$. Unlike the polynomials in $\mathbb{H}[z]$, when substituting an element $z_0 \in \mathbb{H}$ in the two-sided polynomial we follow the two-sided form instead of moving all the coefficients to the left, i.e. $f(z_0) = z_0^n + a_{n-1}z_0^{n-1}b_{n-1} + \dots + a_1z_0b_1 + c$. In [JO10a] Janovská and Opfer provided an example of a quadratic two-sided polynomial with more than two roots with pairwise distinct norms. (These are called essential roots in that paper.)

This is apparently impossible with pure imaginary roots, as the following proposition shows:

PROPOSITION 1.10. *The number of pure imaginary roots of $f(z) = z^2 + azb + c$, assuming $a, b, c \neq 0$, with pairwise distinct norms, is at most two.*

PROOF. Let z_0 be a pure imaginary root of norm N_0 . Therefore $-N_0 + az_0b + c = 0$, i.e. $N_0 - c = az_0b$, hence $a^{-1}b^{-1}N_0 - a^{-1}cb^{-1} = z_0$, which means that $a^{-1}b^{-1}a^{-1}b^{-1}N_0^2 - (a^{-1}b^{-1}a^{-1}cb^{-1} + a^{-1}cb^{-1}a^{-1}b^{-1})N_0 + a^{-1}cb^{-1}a^{-1}cb^{-1} = -N_0$. Consequently, N_0 is a root of the non-trivial polynomial $p(N) = a^{-1}b^{-1}a^{-1}b^{-1}N^2 + (1 - a^{-1}b^{-1}a^{-1}cb^{-1} - a^{-1}cb^{-1}a^{-1}b^{-1})N + a^{-1}cb^{-1}a^{-1}cb^{-1}$. Hence, the number of pure imaginary roots of $f(z)$ with pairwise distinct norms does not exceed 2. \square

2. General Polynomials and Left Eigenvalues

2.1. Polynomial rings over division algebras. Let F be an infinite field and D be a division algebra over F of degree d . We adopt the terminology in [GM65]. Let $D_L[z]$ denote the usual ring of polynomials over D where the variable z commutes with every $y \in D$. When substituting a value we consider the coefficients as though they are placed on the left-hand side of the variable. The substitution

map $S_y : D_L[z] \rightarrow D$ is not a ring homomorphism in general. For example, if $f(z) = az$ and $ay \neq ya$ then $S_y(f^2) = S_y(a^2z^2) = a^2y^2$ while $(S_y(f))^2 = (S_y(az))^2 = (ay)^2 \neq S_y(f^2)$.

The ring $D_G[z]$ is, by definition, the (associative) ring of polynomials over D , where z is assumed to commute with every $y \in F = Z(D)$, but not with arbitrary elements of D . For example, if $y \in D$ is non-central, then yz^2 , zyz and z^2y are distinct elements of this ring. There is a ring epimorphism $D_G[z] \rightarrow D_L[z]$, defined by $z \mapsto z$ and $y \mapsto y$ for every $y \in D$, whose kernel is the ideal generated by the commutators $[y, z]$ ($y \in D$). Unlike the situation of $D_L[z]$, the substitution maps from $D_G[z]$ to D are all ring homomorphisms. Polynomials from $D_G[z]$ are called “general polynomials”, for example $ziz + jzi + zij + 5 \in \mathbb{H}_G[z]$.

Polynomials in $D_L[z]$ and polynomials in $D_G[z]$ which “look like” polynomials in $D_L[z]$, i.e. the coefficients are placed on the left-hand side of the variable, are called “left” or “standard polynomials”, for example $z^2 + iz + j \in \mathbb{H}_G[z]$.

Let $D\langle x_1, \dots, x_N \rangle$ be the ring of multi-variable polynomials, where for every $1 \leq i \leq N$, x_i commutes with every $y \in D$ and is not assumed to commute with x_j for $i \neq j$. This is the group ring of the free monoid $\langle x_1, \dots, x_N \rangle$ over D . The commutative counterpart is $D_L[x_1, \dots, x_N]$, which is the ring of multi-variable polynomials where for every $1 \leq i \leq N$, x_i commutes with every $y \in D$ and with every x_j for $i \neq j$.

For further reading on what is generally known about polynomial equations over division rings see [LS89].

2.2. Left eigenvalues of matrices over division algebras.

Given a matrix $A \in M_n(D)$, a left eigenvalue of A is an element $\lambda \in D$ for which there exists a nonzero vector $v \in D^{n \times 1}$ such that $Av = \lambda v$.

For the special case of $D = \mathbb{H}$ (The algebra of real quaternions) and $n = 2$ it was proven by Wood in [Woo85] that the left eigenvalues of A are the roots of a standard quadratic quaternion polynomial. In [So05] it is proven that for $n = 3$, the left eigenvalues of A are the roots of a general cubic quaternion polynomial.

In [MVPS09], Macías-Virgós and Pereira-Sáez gave another proof for Wood’s result. Their proof makes use of the Study determinant.

Given a matrix $A \in M_n(\mathbb{H})$, there exist unique matrices $B, C \in M_n(\mathbb{C})$ such that $A = B + Cj$. The Study determinant of A is $\det \begin{bmatrix} B & -\overline{C} \\ C & \overline{B} \end{bmatrix}$. The Dieudonné determinant is (in this case) the

square root of the Study determinant. (In [MVPS09] the Study determinant is defined to be what we call the Dieudonné determinant.)

For further information about these determinants see [Asl96].

2.3. The isomorphism between the ring of general polynomials and the group ring of the free monoid with $[D : F]$ variables. Let $N = d^2$, i.e. N is the dimension of D over its center F . In particular there exist $a_1, \dots, a_{N-1} \in D$ such that $D = F + a_1F + \dots + a_{N-1}F$.

Let $h : D_G[z] \rightarrow D\langle x_1, \dots, x_N \rangle$ be the homomorphism for which $h(y) = y$ for all $y \in D$, and $h(z) = x_1 + a_1x_2 + \dots + a_{N-1}x_N$. $D_L[x_1, \dots, x_N]$ is a quotient ring of $D\langle x_1, \dots, x_N \rangle$. Let $g : D\langle x_1, \dots, x_N \rangle \rightarrow D_L[x_1, \dots, x_N]$ be the standard epimorphism.

In [GM65, Theorem 6] it says that if D is a division algebra then the homomorphism $g \circ h : D_G[z] \rightarrow D_L[x_1, \dots, x_N]$ is an epimorphism.

In [Cha12] we proved the following:

THEOREM 2.1. *The homomorphism $h : D_G[z] \rightarrow D\langle x_1, \dots, x_N \rangle$ is an isomorphism, and therefore $D_G[z] \cong D\langle x_1, \dots, x_N \rangle$.*

We also proposed the following algorithm for finding the co-image of x_k for any $1 \leq k \leq N$:

ALGORITHM 2.2. *Let $p_1 = z$, therefore $h(p_1) = x_1 + a_1x_2 + \dots + a_{N-1}x_N$. We shall define a sequence $\{p_j : j = 1, \dots, n\} \subseteq G_1$ as follows: If there exists a monomial in $h(p_j)$ whose coefficient a does not commute with the coefficient of x_k , denoted by c , then we shall define $p_{j+1} = ap_ja^{-1} - p_j$, by which we shall annihilate at least one monomial (the one whose coefficient is a), and yet the element x_k will not be annihilated, because cx_k does not commute with a .*

If c commutes with all the other coefficients then we shall pick some monomial which we want to annihilate. Let b denote its coefficient. Now we shall pick some $a \in D$ which does not commute with cb^{-1} and define $p_{j+1} = bap_jb^{-1}a^{-1} - p_j$.

The element x_k is not annihilated in this process, because if we assume that it does at some point, let us say it is annihilated in $h(p_{j+1})$, then $bacb^{-1}a^{-1} - c = 0$. Therefore $c^{-1}bacb^{-1}a^{-1} = 1$, hence $cb^{-1}a^{-1} = (c^{-1}ba)^{-1} = a^{-1}b^{-1}c$ and, since b commutes with c , a commutes with cb^{-1} and that is a contradiction.

In each iteration the length of $h(p_j)$ (the number of monomials in it) decreases by at least one, and yet the element x_k always remains, and since the length of $h(p_1)$ is finite, this process will end with some p_m for

which $h(p_m)$ is a monomial. In this case, $h(q_m) = cx_k$ and consequently $x_k = h(c^{-1}q_m)$.

2.4. Real Quaternions. Let $D = \mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + ij\mathbb{R}$. Now
 $h(z) = x_1 + x_2i + x_3j + x_4ij$
 $h(z - jzj^{-1}) = h(z + jzj) = 2x_2i + 2x_4ij$
 $h((z + jzj) - ij(z + jzj)(ij)^{-1}) = 2x_2i + 2x_4ij - ij(2x_2i + 2x_4ij)(ij)^{-1} = 4x_2i$
therefore $h^{-1}(x_2) = -\frac{1}{4}i((z + jzj) + ij(z + jzj)ij) = -\frac{1}{4}(iz + ijzj - jzij + zi)$.

Similarly, $h^{-1}(x_1) = \frac{1}{4}(z - izi - jzj - ijzij)$, $h^{-1}(x_3) = -\frac{1}{4}(jz - ijzi + izij + zj)$ and $h^{-1}(x_4) = -\frac{1}{4}(ijz - izj + jzi + zij)$. Consequently, $\bar{z} = \overline{h^{-1}(x_1 + x_2i + x_3j + x_4ij)} = h^{-1}(x_1 - x_2i - x_3j - x_4ij) = -\frac{1}{2}(z + izi + jzj + ijzij)$.

2.5. The characteristic polynomial. Let D, F, d, N be the same as they were in the previous subsection.

There is an injection of D in $M_d(K)$ where K is a maximal subfield of D . (In particular, $[K : F] = d$.) More generally, there is an injection of $M_k(D)$ in $M_{kd}(K)$ for any $k \in \mathbb{N}$. Let \hat{A} denote the image of A in $M_{kd}(K)$ for any $A \in M_k(D)$.

The determinant of \hat{A} is equal to the Dieudonné determinant of A to the power of d . (The reduced norm of A is defined to be the determinant of \hat{A} .)

Therefore $\lambda \in D$ is a left eigenvalue of A if and only if $\det(\widehat{A - \lambda I}) = 0$. Considering D as an F -vector space $D = F + Fa_1 + \cdots + Fa_{N-1}$, we can write $\lambda = x_1 + x_2a_1 + \cdots + x_Na_{N-1}$ for some $x_1, \dots, x_N \in F$. Then $\det(\widehat{A - \lambda I}) \in F[x_1, \dots, x_N]$. It can also be considered as a polynomial in $D\langle x_1, \dots, x_N \rangle$. Now, there is an isomorphism $h : D_G[z] \rightarrow D\langle x_1, \dots, x_N \rangle$, and so $h^{-1}(\det(\widehat{A - \lambda I})) \in D_G[z]$.

Defining $p_A(z) = h^{-1}(\det(\widehat{A - \lambda I}))$ to be the characteristic polynomial of A , the left eigenvalues of A are precisely the roots of $p_A(z)$.

The degree of the characteristic polynomial of A is therefore kd .

REMARK 2.3. If one proves that the Dieudonné determinant of $A - \lambda I$ is the absolute value of some polynomial $q(x_1, \dots, x_N) \in D_L[x_1, \dots, x_N]$ then we will be able to define the characteristic polynomial to be $h^{-1}(q(x_1, \dots, x_N))$ and obtain a characteristic polynomial of degree k .

2.6. The left eigenvalues of a 4×4 quaternion matrix. Let Q be a quaternion division F -algebra. Calculating the roots of the characteristic polynomial as defined in Subsection 2.5 is not always the best way to obtain the left eigenvalues of a given matrix.

The reductions Wood did in [Woo85] and So did in [So05] suggest that in order to obtain the left eigenvalues of a 2×2 or 3×3 matrix one can calculate the roots of a polynomial of degree 2 or 3 respectively, instead of calculating the roots of the characteristic polynomial whose degree is d times greater.

In the next proposition we show how (under a certain condition) the eigenvalues of a 4×4 quaternion matrix can be obtained by calculating the roots of three polynomials of degree 2 and one of degree 6.

In [Cha12] we proved the following:

PROPOSITION 2.4. *If $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ where $A, B, C, D \in M_2(\mathbb{H})$ and C is invertible then λ is a left eigenvalue of M if and only if either $e(\lambda) = f(\lambda)g(\lambda) = 0$ or $e(\lambda) \neq 0$ and $e(\lambda)\overline{e(\lambda)}h(\lambda) - g(\lambda)\overline{e(\lambda)}f(\lambda) = 0$ where $C(A - \lambda I)C^{-1}(D - \lambda I) - CB = \begin{bmatrix} e(\lambda) & f(\lambda) \\ g(\lambda) & h(\lambda) \end{bmatrix}$*

As we saw in Subsection 2.4, $\overline{e(\lambda)}$ is also a quadratic polynomial, which means that $e(\lambda)\overline{e(\lambda)}h(\lambda) - g(\lambda)\overline{e(\lambda)}f(\lambda)$ is a polynomial of degree 6, while the characteristic polynomial of M as defined in Subsection 2.5 is of degree 8.

Bibliography

- [Alb61] A. Adrian Albert, *Structure of algebras*, Revised printing. American Mathematical Society Colloquium Publications, Vol. XXIV, American Mathematical Society, Providence, R.I., 1961. MR 0123587 (23 #A912)
- [ARVT05] Michael Artin, Fernando Rodriguez-Villegas, and John Tate, *On the Jacobians of plane cubics*, Adv. Math. **198** (2005), no. 1, 366–382. MR 2183258 (2006h:14043)
- [Asl96] Helmer Aslaksen, *Quaternionic determinants*, Math. Intelligencer **18** (1996), no. 3, 57–65. MR 1412993 (97j:16028)
- [AY03] Yik-Hoi Au-Yeung, *An explicit solution for the quaternionic equation $x^2 + bx + xc + d = 0$* , Southeast Asian Bull. Math. **26** (2003), no. 5, 717–724. MR 2045106 (2004m:16026)
- [Cha09] Adam Chapman, *Polynomial equations over division rings*, 2009, Thesis (M.Sc.)–Bar-Ilan University.
- [Cha12] ———, *General polynomials over division algebras and left eigenvalues*, Electron. J. Linear Algebra **23** (2012), 508–513. MR 2928573
- [Chi78] Lindsay N. Childs, *Linearizing of n -ic forms and generalized Clifford algebras*, Linear and Multilinear Algebra **5** (1977/78), no. 4, 267–278. MR 0472880 (57 #12567)
- [CK12] Mirela Ciperiani and Daniel Krashen, *Relative Brauer groups of genus 1 curves*, Israel J. Math. **192** (2012), no. 2, 921–949. MR 3009747
- [CKM12] Emre Coskun, Rajesh S. Kulkarni, and Yusuf Mustopa, *On representations of Clifford algebras of ternary cubic forms*, New trends in non-commutative algebra, Contemp. Math., vol. 562, Amer. Math. Soc., Providence, RI, 2012, pp. 91–99. MR 2905555
- [CV12] Adam Chapman and Uzi Vishne, *Clifford algebras of binary homogeneous forms*, J. Algebra **366** (2012), 94–111. MR 2942645
- [CV13] ———, *Square-central elements and standard generators for biquaternion algebras*, Israel J. Math. **197** (2013), no. 1, 409–423. MR 3096621
- [Dic14] L. E. Dickson, *Linear associative algebras and abelian equations*, Trans. Amer. Math. Soc. **15** (1914), no. 1, 31–46. MR 1500963
- [GM65] B. Gordon and T. S. Motzkin, *On the zeros of polynomials over division rings*, Trans. Amer. Math. Soc. **116** (1965), 218–226. MR 0195853 (33 #4050a)
- [Hai84] Darrell E. Haile, *On the Clifford algebra of a binary cubic form*, Amer. J. Math. **106** (1984), no. 6, 1269–1280. MR 765580 (86c:11028)
- [Hai92] ———, *When is the Clifford algebra of a binary cubic form split?*, J. Algebra **146** (1992), no. 2, 514–520. MR 1152918 (93a:11029)
- [Hee54] Nickolas Heerema, *An algebra determined by a binary cubic form*, Duke Math. J. **21** (1954), 423–443. MR 0064030 (16,214d)

- [HH07] Darrell Haile and Ilseop Han, *On an algebra determined by a quartic curve of genus one*, J. Algebra **313** (2007), no. 2, 811–823. MR 2329571 (2008f:16044)
- [HKT09] Darrell Haile, Jung-Miao Kuo, and Jean-Pierre Tignol, *On chains in division algebras of degree 3*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 15-16, 849–852. MR 2542882 (2010h:16039)
- [HS02] Liping Huang and Wasin So, *Quadratic formulas for quaternions*, Appl. Math. Lett. **15** (2002), no. 5, 533–540. MR 1889501 (2003d:12003)
- [JO10a] Drahoslava Janovská and Gerhard Opfer, *The classification and the computation of the zeros of quaternionic, two-sided polynomials*, Numer. Math. **115** (2010), no. 1, 81–100. MR 2594342 (2011b:16096)
- [JO10b] ———, *A note on the computation of all zeros of simple quaternionic polynomials*, SIAM J. Numer. Anal. **48** (2010), no. 1, 244–256. MR 2608368 (2011c:11170)
- [KK12] Cemal Koç and Yosum Kurtulmaz, *Structure theory of central simple \mathbb{Z}_d -graded algebras*, Turkish J. Math. **36** (2012), no. 4, 560–577. MR 2993587
- [KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits. MR 1632779 (2000a:16031)
- [Kuo11] Jung-Miao Kuo, *On an algebra associated to a ternary cubic curve*, J. Algebra **330** (2011), 86–102. MR 2774619 (2012b:16040)
- [Lam73] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Inc., Reading, Mass., 1973, Mathematics Lecture Note Series. MR 0396410 (53 #277)
- [Lon74] F. W. Long, *A generalization of the Brauer group of graded algebras*, Proc. London Math. Soc. (3) **29** (1974), 237–256. MR 0354753 (50 #7230)
- [LS89] J. Lawrence and G. E. Simons, *Equations in division rings—a survey*, Amer. Math. Monthly **96** (1989), no. 3, 220–232. MR 991867 (90g:16015)
- [MRV12] Eliyah Matzri, Louis H. Rowen, and Uzi Vishne, *Non-cyclic algebras with n -central elements*, Proc. Amer. Math. Soc. **140** (2012), no. 2, 513–518. MR 2846319 (2012i:16034)
- [MS82] A. S. Merkur'ev and A. A. Suslin, *K -cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136. MR 675529 (84i:12007)
- [MTW91] P. Mammone, J.-P. Tignol, and A. Wadsworth, *Fields of characteristic 2 with prescribed u -invariants*, Math. Ann. **290** (1991), no. 1, 109–128. MR 1107665 (92g:11035)
- [MV12] Eliyahu Matzri and Uzi Vishne, *Isotropic subspaces in symmetric composition algebras and Kummer subspaces in central simple algebras of degree 3*, Manuscripta Math. **137** (2012), no. 3-4, 497–523. MR 2875290
- [MV14] ———, *Composition algebras and cyclic p -algebras in characteristic 3*, Manuscripta Math. **143** (2014), no. 1-2, 1–18. MR 3147442

- [MVPS09] E. Macías-Virgós and M. J. Pereira-Sáez, *Left eigenvalues of 2×2 symplectic matrices*, Electron. J. Linear Algebra **18** (2009), 274–280. MR 2519914 (2010f:15042)
- [Pap00] Christopher J. Pappacena, *Matrix pencils and a generalized Clifford algebra*, Linear Algebra Appl. **313** (2000), no. 1-3, 1–20. MR 1770355 (2001e:15010)
- [Rac09] Mélanie Raczek, *On ternary cubic forms that determine central simple algebras of degree 3*, J. Algebra **322** (2009), no. 5, 1803–1818. MR 2543635 (2010h:16043)
- [Rev77] Ph. Revoy, *Algèbres de Clifford et algèbres extérieures*, J. Algebra **46** (1977), no. 1, 268–277. MR 0472881 (57 #12568)
- [Rob69] Norbert Roby, *Algèbres de Clifford des formes polynomes*, C. R. Acad. Sci. Paris Sér. A-B **268** (1969), A484–A486. MR 0241454 (39 #2794)
- [Ros99] Markus Rost, *The chain lemma for Kummer elements of degree 3*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 3, 185–190. MR 1674602 (2000c:12003)
- [Row88] Louis H. Rowen, *Ring theory. Vol. II*, Pure and Applied Mathematics, vol. 128, Academic Press Inc., Boston, MA, 1988. MR 945718 (89h:16002)
- [Row92] ———, *Wedderburn’s method and algebraic elements of simple Artinian rings*, Azumaya algebras, actions, and modules (Bloomington, IN, 1990), Contemp. Math., vol. 124, Amer. Math. Soc., Providence, RI, 1992, pp. 179–202. MR 1144036 (92k:16025)
- [Siv12] A. S. Sivatski, *The chain lemma for biquaternion algebras*, J. Algebra **350** (2012), 170–173. MR 2859881 (2012j:16037)
- [So05] Wasin So, *Quaternionic left eigenvalue problem*, Southeast Asian Bull. Math. **29** (2005), no. 3, 555–565. MR 2216293 (2006m:15030)
- [VdB87] M. Van den Bergh, *Linearisations of binary and ternary forms*, J. Algebra **109** (1987), no. 1, 172–183. MR 898344 (88j:11020)
- [Vis02] Uzi Vishne, *Generators of central simple p -algebras of degree 3*, Israel J. Math. **129** (2002), 175–187. MR 1910941 (2003g:16022)
- [Woo85] R. M. W. Wood, *Quaternionic eigenvalues*, Bull. London Math. Soc. **17** (1985), no. 2, 137–138. MR 806238 (86m:15013)